Schriftenreihe der TMF



K. Pommerening | J. Drepper
K. Helbing | T. Ganslandt

Leitfaden zum Datenschutz in medizinischen Forschungsprojekten

Generische Lösungen der TMF 2.0



Medizinisch Wissenschaftliche Verlagsgesellschaft

Schriftenreihe der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.

Band 11

Medizinisch Wissenschaftliche Verlagsgesellschaft

Schriftenreihe der TMF – Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e. V.

Band 11

K. Pommerening | J. Drepper | K. Helbing | T. Ganslandt

Leitfaden zum Datenschutz in medizinischen Forschungsprojekten

Generische Lösungen der TMF 2.0

unter Mitwirkung von
T. Müller, U. Sax, S.C. Semler und R. Speer



Medizinisch Wissenschaftliche Verlagsgesellschaft

Die Autoren

Prof. Dr. Klaus Pommerening
Institut für Medizinische Biometrie,
Epidemiologie und Informatik
Universitätsmedizin der Johannes Gutenberg-Universität Mainz
Obere Zahlbacher Str. 69
55131 Mainz

Dr. Johannes Drepper
TMF – Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e.V.
Charlottenstr. 42
10117 Berlin

Dr. Krister Helbing
Institut für Medizinische Informatik
Universitätsmedizin Göttingen
Robert-Koch-Str. 40
37075 Göttingen

Dr. Thomas Ganslandt
Medizinisches IK-Zentrum
Universitätsklinikum Erlangen
Krankenhausstr. 12
91054 Erlangen

MWV Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG
Zimmerstr. 11
10969 Berlin
www.mwv-berlin.de

ISBN 978-3-95466-295-1 (eBook: PDF)

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Informationen sind im Internet über http://dnb.d-nb.de abrufbar.

© MWV Medizinisch Wissenschaftliche Verlagsgesellschaft Berlin, 2015

Dieses Werk ist einschließlich aller seiner Teile urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Verfasser haben große Mühe darauf verwandt, die fachlichen Inhalte auf den Stand der Wissenschaft bei Drucklegung zu bringen. Dennoch sind Irrtümer oder Druckfehler nie auszuschließen. Daher kann der Verlag für Angaben zum diagnostischen oder therapeutischen Vorgehen (zum Beispiel Dosierungsanweisungen oder Applikationsformen) keine Gewähr übernehmen. Derartige Angaben müssen vom Leser im Einzelfall anhand der Produktinformation der jeweiligen Hersteller und anderer Literaturstellen auf ihre Richtigkeit überprüft werden. Eventuelle Errata zum Download finden Sie jederzeit aktuell auf der Verlags-Website.

Produkt-/Projektmanagement: Frauke Budig, Berlin
Lektorat: Monika Laut-Zimmermann, Berlin
Infografiken: BELAU Werbung und Visuelle Kommunikation
Layout & Satz: eScriptum GmbH & Co KG – Publishing Services, Berlin

Zuschriften und Kritik an:
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG, Zimmerstr. 11, 10969 Berlin, lektorat@mwv-berlin.de

Editorial der TMF

Seit der Gründung der TMF im Jahre 1999 (seinerzeit noch als „Telematikplattform für Medizinische Forschungsnetze") zählt die Auseinandersetzung mit Datenschutzfragen in der biomedizinischen Forschung zu den Hauptaufgaben des Vereins. Und dies zu Recht – stellt doch das deutsche Datenschutzrecht eine bisweilen hohe Hürde bei der Sammlung, Speicherung und Verarbeitung personenbezogener klinischer Daten für Forschungszwecke dar. Mit der Verwendung solcher Daten für die Wissenschaft treten die Verantwortlichen aus dem berufsrechtlich und strafgesetzlich geschützten Bereich der Patientenversorgung heraus. Dies gilt insbesondere bei institutionsübergreifenden Forschungsvorhaben, da solche Projekte in der Regel Patientendaten außerhalb der jeweils behandelnden Institutionen zusammenführen müssen. Erstreckt sich das Vorhaben dann noch über mehrere Bundesländer, so bekommen die Forscher es unter Umständen mit einer Vielzahl spezialgesetzlicher Vorgaben und der Zuständigkeit unterschiedlicher Aufsichtsbehörden zu tun. Für Wissenschaftler mit notorisch engem Finanz- und Zeitbudget ist es daher wichtig, die datenschutzrechtlichen Anforderungen genau zu kennen und Werkzeuge für ihre Erfüllung zur Hand zu haben, um so möglichst schnell grünes Licht für ihre Projekte durch die Aufsichtsstellen erhalten zu können.

Vor diesem Hintergrund haben sich Wissenschaftler in der TMF schon vor vielen Jahren zu einer interdisziplinären Arbeitsgruppe zusammengeschlossen, um gemeinsam mit Vertretern der Datenschutzbehörden in den Jahren 2001 bis 2003 eine „Blaupause" für die rechtskonforme Verarbeitung medizinischer Daten in unterschiedlichen Forschungskontexten zu entwickeln. Diese 2003 vorgelegten „Generischen Datenschutzkonzepte" bilden mit ihren beiden Modellen A und B bis heute die Grundlage für ein standardisiertes Vorgehen hinsichtlich Datensicherheit und Schutz der informationellen Selbstbestimmung in der biomedizinischen Forschung. Daneben dienten die Konzepte der TMF auch als Grundlage für die Spezifikationen diverser Software-Werkzeuge für die praktische Umsetzung datenschutzrechtlicher Vorgaben in den IT-Architekturen von Forschungsprojekten.

Der Erfolg der „Generischen Datenschutzkonzepte" dokumentierte sich jedoch vor allem in einem seinerzeit mit den Datenschutzbeauftragten abgestimmten Verfahren, das 2003 auch im Vorwort des Koordinierungsrates (heute: Vorstand) der TMF zur Druckversion beschrieben wurde. Danach sollten die „Generischen Datenschutzkonzepte" als Grundlage für die Erstellung spezifischer Sicherheitspolicies und Datenmanagementkonzepte der einzelnen Netze bzw. Projekte dienen, um auf diese Weise die Genehmigungsverfahren durch die Landesdatenschutzbeauftragten zu beschleunigen. Das Ergebnis spricht für sich: Eine Vielzahl von Forschungsverbünden hat seit 2003 seine Datenschutzkonzepte erfolgreich an den generischen Vorschlägen der TMF ausgerichtet, und über 80 Forschungsprojekte haben sich durch die Arbeitsgruppe (AG)

Datenschutz der TMF, die sich zunehmend als zentrale Anlaufstelle für Datenschutzfragen in der biomedizinischen Forschung etabliert hat, beraten lassen. Auch die Verständigung auf eine gemeinsame Sprache und die Darlegung der gegenseitigen Ansprüche trugen zu einer deutlichen Verschlankung und Verkürzung der Genehmigungsverfahren bei, was allen Beteiligten Zeit und Arbeit erspart – und somit zweifellos auch einen volkswirtschaftlichen Nutzen hat.

Die „Generischen Datenschutzkonzepte" der TMF haben zweierlei bewirkt: Zum einen ist es durch sie gelungen, in Datenschutzfragen einen Community-Konsens der Anwender, d.h. der Ärzte und Nicht-Ärzte, in den Forschungsverbünden herzustellen. Darüber hinaus wurde jedoch auch ein sehr fruchtbarer Dialog mit den Datenschutzbeauftragten der Länder und des Bundes angestoßen, der bis heute anhält. Aus einst versteckt (oftmals auch offen) empfundener Gegnerschaft ist eine Partnerschaft in der Sache geworden. Nicht zuletzt muss ja auch die Forschung ein großes Interesse daran haben, durch nachweislich datenschutzgerechte Verfahren jenes Vertrauen bei ihren Patienten und Probanden aufzubauen und zu erhalten, das die unerlässliche Grundlage für deren freiwillige Mitwirkung an medizinischen Forschungsprojekten bildet.

2003 wurde die erste Version der „Generischen Datenschutzkonzepte" digital veröffentlicht; 2006 erfolgte die Buchpublikation als Band 1 in der Schriftenreihe der TMF (Carl-Michael Reng, Peter Debold, Christof Specker, Klaus Pommerening: „Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin". MWV, Berlin, 2006). Doch Datenschutzkonzepte können niemals statisch sein. Technische Weiterentwicklungen (z.B. in der Kryptographie und in der IT-Sicherheit) und Änderungen der rechtlichen Rahmenbedingungen (siehe die aktuellen Planungen für ein harmonisiertes EU-Datenschutzrecht) verändern die Anforderungen an den Datenschutz ebenso wie neue wissenschaftliche Errungenschaften (z.B. das Next Generation Sequencing) und soziale Entwicklungen (z.B. die Verbreitung der Social Media Netzwerke). Auch muss der Diskurs zwischen theoretischen Datenschutzanforderungen und vertretbarem Realisierungsaufwand – vor allem vor dem Hintergrund des internationalen Wettbewerbs in der biomedizinischen Forschung – stets neu geführt werden. Daher bedurfte es stets einer regelmäßigen Fortschreibung der „Generischen Datenschutzkonzepte", und schon 2006 gab es die erste Erweiterung um den Bereich der Biobanken, die allerdings nur digital zur Verfügung steht.

Zum Jahreswechsel 2005/2006 begann schließlich die Planung eines TMF-finanzierten Projekts zur umfassenden Revision und Erweiterung der „Generischen Datenschutzkonzepte". Dieses Vorhaben (Revision der generischen Datenschutzkonzepte der TMF, D039-03) konnte im Sommer 2006 unter der bewährten Leitung von Prof. Dr. Klaus Pommerening (von 1999 bis heute Sprecher der AG Datenschutz der TMF) gestartet werden. Nach langer intensiver Arbeit wurde im Sommer 2013 eine neue Version der „Generischen Daten-

schutzkonzepte“ der TMF vorgelegt, die sich in vielem von der Vorgängerfassung unterscheidet. Insbesondere ist es den Verfassern gelungen, die Konzepte geeignet zu modularisieren, so dass jetzt je nach Art eines Forschungsprojekts unterschiedliche Komponenten gezielt genutzt werden können. Auch wurden „Lesehilfen“ erstellt, die eine leichtere punktuelle Nutzung der Konzepte ermöglichen – von beispielhaften Anwendungsfällen über Vergleiche der alten und neuen Fassungen bis hin zu nützlichen Begriffserklärungen im Glossar.

Die neue Version der „Generischen Datenschutzkonzepte“ wurde ebenfalls mit den Datenschutzbeauftragten der Länder und des Bundes, vertreten durch ihre Arbeitskreise Wissenschaft (Leitung: Dr. Rita Wellbrock, LfD Hessen) und Technik (Leitung: Gabriel Schulz, LfDI Mecklenburg-Vorpommern), abgestimmt. In konstruktiver Zusammenarbeit wurde dabei intensiv um Formulierungen und Inhalte gerungen, um die Vorstellungen auf Seiten der Aufsichtsbehörden mit den Realisierungsmöglichkeiten auf Seiten der Forscher in Einklang zu bringen. Am 27./28. März 2014 wurde die finale Fassung schließlich auf der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder angenommen und zur Nutzung in der medizinischen Forschung empfohlen. Die TMF freut sich, die „Version 2.0“ der „Generischen Datenschutzkonzepte“ nun unter dem Titel „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten“ als weiteren Meilenstein für die vernetzte medizinische Forschung in ihrer Schriftenreihe zur Verfügung stellen zu können.

Um das Gelingen dieses schwierigen Werks haben sich im Laufe von anderthalb Dekaden viele engagierte Wissenschaftler und Experten verdient gemacht.

Für ihre grundlegenden Arbeiten an den „Generischen Datenschutzkonzepten“ in der Version 1 gilt den Autoren PD Dr. Michael Reng und Prof. Dr. Klaus Pommerening sowie Dr. Peter Debold, Prof. Dr. Christof Specker und PD Dr. Klaus Adelhard unvermindert Dank dafür, dass sie ihre jeweilige Kompetenz als Arzt, Forscher bzw. IT- und Sicherheitsexperte eingebracht haben. Auf den in der Version 1 beschriebenen Modellen A und B beruhen das klinische Modul bzw. das Forschungsmodul im jetzt vorgelegten Leitfaden. Auch dem Koordinierungsrat der TMF der Jahre 2001–2003 (damals geleitet von Prof. Dr. Otto Rienhoff) ist für Initiierung des Projekts zu danken, ebenso dem Bundesministerium für Bildung und Forschung (BMBF) für die Unterstützung dieser und der meisten der nachfolgend genannten Aktivitäten der TMF. Schon in der Frühphase der Arbeit an den Konzepten haben Vertreter der Landesdatenschutzbeauftragten wichtige Beiträge hierzu geleistet. Insbesondere sind die Vorsitzende des Arbeitskreises Wissenschaft der Landesbeauftragten für Datenschutz, Dr. Rita Wellbrock (Hessen), und der frühere Landesdatenschutzbeauftragte des Landes Bayern, Reinhard Vetter, zu nennen, die die Idee eines zwischen Forschern und Datenschützern abgestimmten Grundkonzepts entscheidend unterstützt haben.

Die Erweiterung um ein generisches Datenschutzkonzept für Biobanken wurde 2004 bis 2006 durch die Arbeitsgruppe Biomaterialbanken (BMB) der TMF initiiert und von einer interdisziplinären Projektgruppe bearbeitet. Hieran beteiligt waren Prof. Dr. Klaus Pommerening, PD Dr. Michael Hummel, Prof. Dr. Michael Krawczak, Prof. Dr. Jürgen W. Goebel, PD Dr. Dr. Michael Kiehntopf und Peter Ihle sowie aus der TMF-Geschäftsstelle Dr. Regina Becker, Sebastian C. Semler und Eva Sellge. Eine wichtige Grundlage dieser Arbeiten bildete das 2006 veröffentlichte und von der Projektgruppe begleitete Rechtsgutachten durch Prof. Dr. Jürgen Simon et al., das als Band 2 in der TMF-Schriftenreihe publiziert ist.

Für ihre immense fachliche und organisatorische Arbeit im Rahmen der Revision und der Erstellung des neuen Leitfadens ist insbesondere den Autoren Prof. Dr. Klaus Pommerening (Mainz) und Dr. Johannes Drepper (TMF-Geschäftsstelle) sowie Dr. Krister Helbing (Universität Göttingen bzw. TMF-Geschäftsstelle), Dr. Thomas Ganslandt (Erlangen) und der beteiligten Projektgruppe (Prof. Dr. Ulrich Sax, Göttingen, Ronald Speer, Leipzig, Dr. Thomas Müller, München, und Sebastian C. Semler, TMF-Geschäftsstelle) zu danken. Auch in den Leitfaden flossen wesentliche Erkenntnisse aus Rechtsgutachten ein, die die TMF in den vergangenen Jahren beauftragt, begleitet und veröffentlicht hat. Insbesondere zu nennen sind hier die Gutachten von Prof. Dr. Dr. Christian Dierks (RA Kanzlei Dierks & Bohle, Berlin) zur Treuhänderschaft und Pseudonymisierungspflicht in klinischen Studien sowie das Rechtsgutachten von Prof. Dr. Alexander Roßnagel, Prof. Dr. Gerrit Hornung und Dr. Silke Jandt (Kassel) zur Nutzbarkeit von Versorgungsdaten und der elektronischen Gesundheitskarte für Forschungszwecke. Beide Gutachten wurden zudem von Claus Burgardt (RA Kanzlei Sträter, Bonn) gesichtet und kommentiert. Die Gutachten sind online über die Webseite der TMF verfügbar.

Wie zuvor sind wir auch im Zusammenhang mit der Revision der Generischen Datenschutzkonzepte den Datenschutzbeauftragten, namentlich den Arbeitskreisen Wissenschaft und Technik, für ihre engagierte Diskussion und Kommentierung sowie für die abschließende Zustimmung dankbar. Unser besonderer Dank gilt einmal mehr Frau Dr. Wellbrock (LfD Hessen), die den Abstimmungsprozess koordinierte. Daneben verdanken wir Jutta Katernberg (LfDI Nordrhein-Westfalen), Hendrik Wilmsmeyer (LfDI Nordrhein-Westfalen), Matthias Jaster (LfDI Hamburg), Wilhelm Kaimaier (LfD Niedersachsen) und Dr. Ulrich Vollmer (LfDI Berlin) viele wichtige Hinweise und Anregungen.

Besonders zu danken ist der AG Datenschutz der TMF und den vielen Wissenschaftlern, die ihre Projekte zwecks Beratung in der AG vorgestellt haben. Durch sie ist ein einzigartiger Überblick über die biomedizinische Forschungslandschaft und die dort relevanten Datenschutzbelange entstanden. Gerade die Diskussion mit den praktisch Betroffenen hat in den vergangenen elf Jahren maßgeblich zu dem Erkenntnisfortschritt beigetragen, der sich in der Revision niedergeschlagen hat. Insbesondere sei in diesem Zusammenhang

Gisela Antony (Marburg) und Prof. Dr. Norbert Graf (Homburg) gedankt, die viele Anwendungsfälle und Fallbeispiele zum vorliegenden Band beigetragen haben.

Der TMF-Geschäftsstelle gilt unser Dank für ihre kontinuierliche Organisationsunterstützung der AG Datenschutz und der beteiligten TMF-Projekte. Im Zusammenhang mit der vorliegenden Publikation in Buchform danken wir insbesondere Antje Schütt für das Lektorat und Dr. Elke Witt für die Aufbereitung der Literatur.

Im Laufe der Jahre ist mit den „Generischen Datenschutzkonzepten" der TMF und den darauf basierenden Software-Werkzeugen der praktische Nachweis gelungen, dass eine rechtskonforme Umsetzung des Datenschutzes in der medizinischen Forschung technisch und organisatorisch möglich ist. Die TMF hofft, dass die „Generischen Datenschutzkonzepte" auch in ihrer revidierten Fassung einen vielfältigen Nutzen bei der Bewältigung der „Hürde Datenschutz" durch die biomedizinische Forschung entfalten mögen. Zugleich bitten wir alle Beteiligten darum, den Erfahrungsaustausch fortzusetzen, Best Practice-Erkenntnisse zu sammeln und der TMF hierzu ein kontinuierliches Feedback zu geben. Nur so lässt sich auch künftigen Herausforderungen auf diesem Feld geeignet begegnen. Die AG Datenschutz der TMF wird der biomedizinischen Forschung auch in Zukunft gern als Ansprechpartner zur Verfügung stehen.

Für die TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) im Auftrag des Vorstands

Sebastian Claudius Semler
(Geschäftsführer)

Prof. Dr. Michael Krawczak
(Vorstandsvorsitzender)

Die 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg empfiehlt medizinischen Forschungseinrichtungen und Forschungsverbünden, den von der TMF entwickelten „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF – Version 2“ (Dokumentversion 1.01) als Basis zu nehmen für die konkrete Ausgestaltung ihrer Datenschutzkonzepte (siehe http://www.datenschutz.hessen.de/dg011.htm#entry4196).

Der mit diesem Buch vorgelegte Text stellt eine endredaktionell überarbeitete Fassung des der Empfehlung der Konferenz der Datenschutzbeauftragten zugrundeliegenden Dokuments dar. Inhaltliche Änderungen wurden nicht vorgenommen, lediglich die Fußnoten 14 und 17, Quellenhinweise im Glossar sowie das Kapitel 7 „Zusammenfassung und Ausblick“ wurden im Zuge der Überarbeitung noch ergänzt. Zudem war der Inhalt des elektronischen Anhangs nicht Gegenstand des Abstimmungsprozesses zwischen der TMF und den Datenschutzbeauftragten und ist somit von der Empfehlung nicht mit umfasst.

Inhalt

1 Einführung

Die medizinische Forschung arbeitet zunehmend vernetzt in immer größeren Forschungsverbünden. Um international konkurrenzfähig zu bleiben – und in manchen Gebieten: wieder zu werden – wird vorrangig die landesweite Bündelung von Kompetenzen als nötig erachtet. Daher unterstützen das Bundesministerium für Bildung und Forschung (BMBF) und die Deutsche Forschungsgemeinschaft (DFG) seit einigen Jahren mit Nachdruck den Aufbau der vernetzten Forschung; zu erwähnen sind vor allem die Kompetenznetze in der Medizin[1], die Transregio-Sonderforschungsbereiche, die Netzwerke für seltene Erkrankungen, das Nationale Genomforschungsnetz, die Nationale Biobanken-Initiative und nicht zuletzt auch die Deutschen Zentren der Gesundheitsforschung[2]. Auch die zunehmend geforderte europäische Ausrichtung von Forschungsprojekten verdeutlicht den Vernetzungsdruck im biomedizinischen Forschungsbereich.

Die Vernetzung schafft überregionale, meist auf die Erforschung bestimmter Krankheiten ausgerichtete Kooperationen von Grundlagenforschern und Klinikern, die durch gemeinsame Ressourcen-Nutzung Synergien freisetzen. Ein wichtiges Element dieser Kooperation ist die überregionale Zusammenführung und Bereitstellung aller forschungsrelevanten Daten in zentralen Daten-

1 http://www.kompetenznetze-medizin.de
2 http://www.bmbf.de/de/gesundheitszentren.php

banken bzw. Registern und von Proben in zentralen Biobanken. Wie solche Datenbanken und Probensammlungen datenschutzgerecht aufgebaut, organisiert und betrieben werden können, wird in dem vorliegenden Text beschrieben und in Abbildung 1 illustriert.

Das nachfolgende Kapitel 2 erläutert, wie ein generisches Konzept als Blaupause eines konkreten Datenschutzkonzepts für einen bestimmten Forschungsverbund verwendet werden kann. Auch die Unterschiede zwischen den ersten Modelllösungen der TMF aus dem Jahr 2003 [1] und der jetzt vorgelegten Revision sowie die Verzahnung mit dem bis 2006 weiterentwickelten generischen Datenschutzkonzept für Biobanken [2] sind in diesem Kapitel beschrieben.

In Kapitel 3 wird der Anwendungsbezug dieses Datenschutzkonzepts hervorgehoben. Beispielhaft geschilderte Anwendungsfälle erleichtern gerade Praktikern der medizinischen Forschung den Einstieg in die Thematik und erlauben eine erste Einschätzung, welche Module des Gesamtkonzepts für einen konkreten Einsatz in eigenen Projekten von Interesse sein könnten.

Kapitel 4 widmet sich den datenschutzrechtlichen Grundlagen für den Aufbau und die Nutzung zentraler Daten- und Probeninfrastrukturen in der medizinischen Verbundforschung. Aufgrund der Komplexität der Materie kann nur ein erster Überblick gegeben werden, um den Einstieg zu erleichtern. Für den interessierten Leser wird jedoch auch auf weiterführende Literatur verwiesen, wie z.B. die zu verschiedenen Themen im Auftrag der TMF erstellten Rechtsgutachten.

Einen konkreten Einblick in die Modelllösungen für verschiedene Aufgabenstellungen und Anwendungsszenarien der Verbundforschung bietet Kapitel 5. Im Unterschied zu den bisherigen generischen Lösungen der TMF ist das vorliegende Konzept modular aufgebaut, was sich auch in der Kapitelstruktur widerspiegelt: Jedes Modul ist in einem eigenen Unterkapitel dargestellt, wobei auch Bezüge zum Anwendungsfall und konkrete Hinweise zur Realisierung zur Sprache kommen.

Übergreifende Aspekte, die für alle Module relevant sind, und beispielhafte Verknüpfungen verschiedener Module bis hin zu einem Maximalmodell eines Forschungsverbunds werden in Kapitel 6 aufgegriffen. Somit stellen die Kapitel 5 und 6 das Herzstück der vorliegenden modellhaften Datenschutzkonzepte dar. Kapitel 5 erlaubt jedoch aufgrund der modularen Ausrichtung ein selektives Lesen der relevanten Unterkapitel.

Nach einer zusammenfassenden Darstellung samt Ausblick in Kapitel 7 findet sich ein umfassendes Glossar, welches alle relevanten verwendeten Begriffe dieses Leitfadens eindeutig erklärt und erläutert. Ein wichtiges Ziel des Glossars ist die Vermeidung von Missverständnissen, die häufig auf unterschiedliche Interpretationen komplexer Begrifflichkeiten zurückgehen.

Zur konkreten Unterstützung bei der Konzeption und Umsetzung eines eigenen Datenschutzkonzepts findet sich in einem online zur Verfügung gestellten Anhang[3] eine Übersicht über verfügbare und ggf. nach Anpassung einsetzbare Dokumente. Hierzu gehören Checklisten, Vertragsvorlagen, Policies, Vorlagen für Standard Operating Procedures (SOP) und Ähnliches.

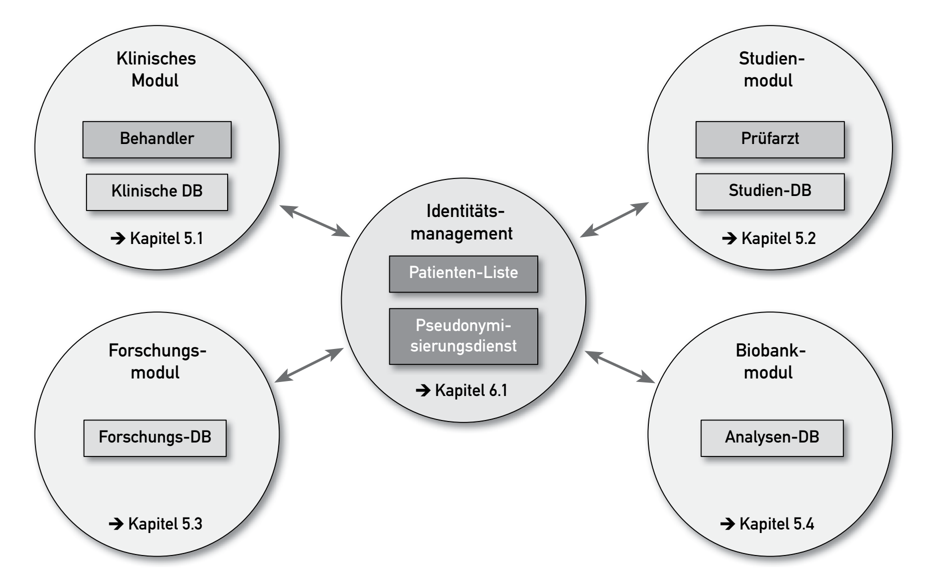


Abb. 1 Übersicht über die Module und modulverbindende zentrale Komponenten des neuen Datenschutzkonzepts mit Verweisen auf die jeweiligen Kapitel mit ausführlichen Beschreibungen

3 siehe www.tmf-ev.de/datenschutz-leitfaden

2 Datenschutzkonzepte der TMF

In der Arbeitsgruppe Datenschutz der TMF wurden in den letzten zehn Jahren über 80 Forschungsprojekte in Bezug auf eine datenschutzgerechte Umsetzung von Daten- und Probensammlungen beraten. Grundlage der Beratung waren die generischen Datenschutzkonzepte der TMF, die 2003 mit den Arbeitskreisen „Wissenschaft und Forschung“ und „Gesundheit und Soziales“ der Datenschutzbeauftragten des Bundes und der Länder auf nationaler Ebene abgestimmt und 2006 in der Schriftenreihe der TMF in Buchform veröffentlicht wurden [1]. Mit diesen generischen Lösungen ist erstmals der Versuch gemacht worden, sowohl die Erstellung formal akzeptabler und bundesweit einsetzbarer Datenschutzkonzepte für unterschiedlichste Verbundforschungsprojekte als auch den damit verbundenen Prüfungs- und Abstimmungsprozess mit Ethikkommissionen und Datenschützern deutlich zu vereinfachen und zu beschleunigen. Insbesondere an der Notwendigkeit, im Rahmen der Erstellung und Abstimmung eines konkreten Datenschutzkonzepts medizinische, informationstechnische, juristische und organisatorische Kompetenz zu bündeln, sind früher viele Forschungsprojekte gescheitert. Die Bereitstellung eines generischen Konzepts sollte hier Abhilfe schaffen. Dieses war sowohl als Ausgangspunkt eigener Dokumente wie auch als Einführung in und Anleitung für das komplexe Themenfeld gedacht.

Die generischen Datenschutzkonzepte sind in den letzten Jahren zweifellos eines der bekanntesten, wichtigsten und erfolgreichsten Produkte der TMF

geworden. Sie werden mittlerweile auch weit über die Mitgliedschaft der TMF hinaus genutzt und angewendet. Die Konzepte haben für die Verbundforschung neue Möglichkeiten geschaffen und hierfür bundesweit einen einheitlichen und breit akzeptierten Bezugsrahmen für die Abstimmung mit den Datenschützern aufgespannt. Die Begleitung der Erstellung und Abstimmung von konkreten Datenschutzkonzepten durch die Arbeitsgruppe Datenschutz der TMF hat gezeigt, dass die Zeit bis zu einer abschließenden Stellungnahme der Datenschützer (und damit die Wartezeit bis zum eigentlichen Start der Daten- und Probensammlung) deutlich verkürzt werden konnte. Kostenaufwändige technische und juristische „Wieder-Erfindungen" einerseits sowie auch das Verfolgen bereits primär unzureichender Lösungen andererseits konnte für eine Reihe von Forschungsprojekten verhindert werden.

Die Modelllösungen der TMF haben Wege aufgezeigt, wie sachgerecht mit Patientendaten umgegangen und gleichzeitig ein für die Forschung relevanter Datensatz verfügbar gemacht werden kann. Dabei wurde zwischen dem Modell A für Forschungsnetze mit „klinischem Fokus" und dem Modell B für eher „wissenschaftlich orientierte" Netze unterschieden. Diese Lösungen werden mit der vorliegenden Ausarbeitung aufgrund der zwischenzeitlich gemachten Erfahrungen fortgeschrieben, aktualisiert und erweitert. Grundlage war und ist die sorgfältige Abwägung von Rechtsgütern, die im Auftrag der TMF von führenden Medizin- und Datenschutzrechtlern durch Gutachten unterstützt wurde. Eingesetzt wird das Instrumentarium, das die Datenschutzgesetze zur Wahrung der Persönlichkeitsrechte anbieten: Patientenaufklärung und -einwilligung, Anonymisierung und Pseudonymisierung, informationelle Gewaltenteilung und Datentreuhänderschaft, organisatorische Maßnahmen und vertragliche Regelungen sowie die sichere Gestaltung der informationstechnischen Infrastruktur.

Das erarbeitete Konzept mit seinen Varianten wird den Belangen der Patienten – und der in vielen Forschungsprojekten auch benötigten gesunden Probanden – ebenso gerecht wie den Anforderungen der medizinischen Forschung, und es minimiert die Rechtsgüterkonflikte.

2.1 Das Prinzip eines generischen Datenschutzkonzepts

Das vorliegende Konzept zeigt verschiedene Wege zum datenschutzgerechten Aufbau medizinischer Forschungsverbünde auf. Es verfolgt einen modularen und skalierbaren Ansatz, der verschiedene Schwerpunkte zulässt und den Anforderungen von versorgungsnaher Forschung, klinischen Studien, epidemiologischen Projekten, Biobanken, Registern und Langzeitforschungsprojekten gerecht wird. Es waren widersprüchliche Zielvorstellungen zu harmonisieren: Möglichst vielfältige Anforderungen der medizinischen Verbundforschung sollten abgedeckt und dabei doch die Datenprozessierung so konkret wie möglich definiert werden. Das generische Konzept soll und muss den Forschungs-

verbünden helfen, möglichst einfach und schnell zu einem spezifischen Datenschutzkonzept zu kommen, das dem zuständigen Datenschutzbeauftragten alle zur Beurteilung nötigen Informationen liefert. Durch den modularen Aufbau kommt das Konzept diesen Zielen gleichzeitig sehr nahe und integriert dabei die Modelllösungen A und B des „alten“ Konzepts als eigene Module.

Die erarbeiteten Modelllösungen werden in unterschiedlichen Forschungsverbünden mit unterschiedlicher Zusammenstellung der Module bis hin zum „Maximalmodell“ bereits eingesetzt. Weitere Verbünde sind in der Planung weit fortgeschritten. Die Beratung durch die Arbeitsgruppe Datenschutz der TMF soll dabei helfen, ein konsensfähiges konkretes Datenschutzkonzept auf der Basis der generischen Vorlage zu erarbeiten.

2.2 Unterschiede zur bisherigen Version der generischen Datenschutzkonzepte

Das „alte“ Konzept war auf die schnelle Erfüllung dringender Anforderungen hin verfasst worden. Unvollständigkeit wurde bewusst in Kauf genommen und als solche kenntlich gemacht. Der Auftrag zur Fortschreibung ist explizit formuliert worden. Schon 2005 wurden in einem Workshop der TMF systematisch die Erfahrungen mit diesem Ansatz gesammelt und der Revisionsbedarf konkretisiert. Im Einzelnen wurden als zu berücksichtigende Themenbereiche und Gesichtspunkte herausgearbeitet:

- Der „klinische“ bzw. „wissenschaftliche“ Fokus war das wesentliche Unterscheidungsmerkmal der Modelle A und B. Dies ist aber keine Eigenschaft eines Forschungsverbundes, sondern eine Eigenschaft eines Einzelprojekts, einer Datenbank oder Datensammlung. In einem großen Verbund sind in der Regel beide Aspekte gleichzeitig von Bedeutung. Diese Änderung der Sichtweise gegenüber dem alten Konzept führte dazu, dass die Modelle A und B unter einem gemeinsamen Dach zusammenzufassen und auch in ihrem Wechselspiel zu beleuchten waren.
- Die Erfahrungen mit der bisherigen Umsetzung in Forschungsverbünden zeigten auch konkret, dass die Dichotomie zwischen den Modellen A und B oft nur mühevoll mit den Anforderungen der Praxis in Übereinstimmung zu bringen war.
- Der Bereich der klinischen Studien war im alten Konzept bewusst ausgeklammert worden, auch weil die gesetzlichen Grundlagen dafür noch in der Diskussion waren. Sie sind inzwischen in Neufassungen des Arzneimittelgesetzes (AMG) und des Medizinproduktegesetzes (MPG) festgeschrieben. Da selbstverständlich in den meisten Forschungsverbünden solche Studien eine zentrale Rolle spielen, musste dieser Bereich im revidierten Konzept ebenfalls behandelt und auch seine Querverbindungen mit anderen Forschungsprojekten des Verbunds dargestellt werden.

- Mit den Gesetzen zur Gesundheitsreform und den Bestrebungen, die Gesundheitstelematik flächendeckend voranzubringen, wurden neue gesetzliche Rahmenbedingungen mit Konsequenzen für die Nutzung von Versorgungsdaten für die Forschung definiert. Andererseits wächst in der Forschergemeinde die Einsicht in die Notwendigkeit, „Routinedaten“ aus der Krankenversorgung für die medizinische Forschung zu nutzen, ein Thema, dem sich auch die TMF in verschiedenen Projekten gestellt hat. Eine Reihe nationaler [3] und internationaler [4] Projekte zeigt die Möglichkeiten dieses Ansatzes.
- Die Abgrenzung von Forschung und Versorgung und andere inzwischen aufgeworfene rechtliche Fragen wurden von der TMF aufgegriffen und systematisch im Rahmen von Rechtsgutachten führender Experten aufgearbeitet. Die Ergebnisse dieser Gutachten waren in das Datenschutzkonzept einzuarbeiten.
- Auch die Einbindung des zwischenzeitlich entstandenen Datenschutzkonzepts für Biomaterialbanken in den Gesamtrahmen musste dargestellt werden.

Aus diesen Gründen schien es wenig zweckmäßig, nur den vorhandenen Text zu überarbeiten. Vielmehr musste der Ansatz hin zu einem modularen und flexiblen Gesamtkonzept geändert werden, was mit einer systematischen Aufarbeitung von Grund auf verbunden war. Dadurch weicht die revidierte Version textlich sehr weit von der alten Version ab. Das heißt jedoch nicht, dass diese völlig verworfen werden muss: Ein großer Teil der grundsätzlichen Überlegungen ist nach wie vor gültig, und beide alten Modelle werden inhaltlich weiterhin vollständig abgedeckt. Sie finden sich in den Modulen „Klinisches Modul“ und „Forschungsmodul“ wieder. Das Datenschutzkonzept für Biomaterialbanken bleibt weiterhin gültig und wird über das „Biobankenmodul“ in das Gesamtkonzept eingebunden. Abbildung 2 zeigt auf einen Blick, wie die bisherigen Konzepte in das neue Gesamtkonzept integriert wurden. Genauer ist die Einbindung in die neue übergreifende Struktur im Kapitel 6.1.7 und insbesondere in den dort stehenden Abbildungen 15–17 illustriert.

2.3 Anwendung dieses Leitfadens

Der Anwendungsbereich dieses Leitfadens und des darin vorgezeichneten generischen Konzepts ist in erster Linie der Aufbau eines oder mehrerer Datenpools – auch in Kombination mit einer oder mehreren Biobanken – in einem medizinischen Forschungsverbund. Ergänzend ist die von der TMF erarbeitete Checkliste für die Patientenaufklärung und Einwilligung [5] sowie das generische Datenschutzkonzept für Biomaterialbanken [2] zu berücksichtigen. Aufbauend auf den bisherigen Empfehlungen zur Nutzung der TMF-Datenschutzkonzepte [1, S. 88] und den in der Arbeitsgruppe mittlerweile gemachten Erfahrungen wird das nachfolgend beschriebene Vorgehen vorgeschlagen, das

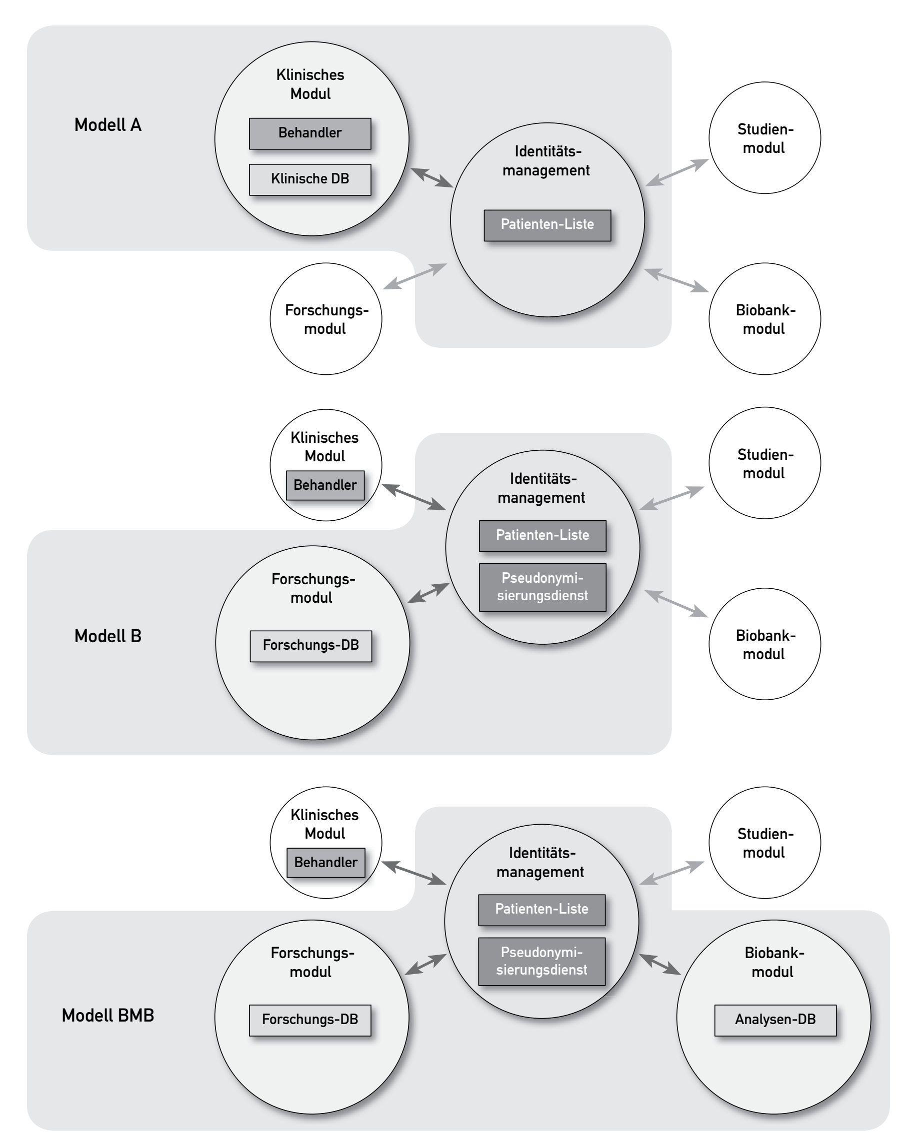


Abb. 2 Integration der bisherigen generischen Datenschutzkonzepte der TMF in die vorliegende modulare Konzeption. In der Abbildung der Modelle B und BMB ist für die Dateneingabe der Behandler aus dem Klinischen Modul nur beispielhaft dargestellt.

mit den Datenschützern auf Landes- und Bundesebene abgestimmt ist und die neu vorgelegte modulare Modellkonzeption berücksichtigt:

1. Für die Erstellung eines Datenschutzkonzepts sollten zunächst die Anwendungsfälle und die sich daraus ergebenden Anforderungen geklärt werden. Auf Basis dieser Analyse können die notwendigen Module (s. Kap. 5) bestimmt und ggf. auch ergänzende technische und organisatorische Maßnahmen festgelegt werden.
2. Bei der Erstellung eines Datenschutzkonzepts für ein Forschungsprojekt sollten die technischen und organisatorischen Prinzipien der relevanten Module aus Kapitel 5 und der allgemeinen Maßnahmen aus Kapitel 6 möglichst weitgehend übernommen werden. Abweichungen müssen gut begründet sein.
3. Bei der Überarbeitung bereits bestehender Datenschutzkonzepte ist zu prüfen, inwieweit die hier beschriebenen Prinzipien übernommen werden können.
4. Die erste schriftliche Version eines Datenschutzkonzepts wird von dem zuständigen Mitarbeiter der Forschungseinrichtung oder des Verbunds der Arbeitsgruppe Datenschutz der TMF vorgestellt, so dass Empfehlungen aus diesem Kreis vor einer Finalisierung eingearbeitet werden können. Zur Klärung der Sitzungstermine und der zugehörigen Einreichungsfristen ist die Geschäftsstelle der TMF zu kontaktieren.
5. Ein Datenschutzkonzept, das aus Sicht der Arbeitsgruppe Datenschutz der Überarbeitung bedarf, kann dieser in revidierter Form erneut zur Prüfung vorgelegt werden.
6. Die Arbeitsgruppe Datenschutz fasst nach Prüfung und Diskussion den Beschluss, ob das Datenschutzkonzept in der vorliegenden Form aus Sicht der TMF akzeptiert werden kann und formuliert im positiven Falle – ggf. mit Änderungs- und Ergänzungsvorschlägen – eine Stellungnahme, die insbesondere auf die Abweichungen von der hier vorgelegten generischen Konzeption eingeht.

Die vorliegenden Empfehlungen für eine datenschutzgerechte Verwendung von Patientendaten in der medizinischen Forschung sind inhaltlich mit den Aufsichtsbehörden im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder abgestimmt. Der Leitfaden stellt mithin einen Rahmen dar, an dem sich Forschungseinrichtungen und Verbundforschungsprojekte bei der Erstellung von Datenschutzkonzepten orientieren sollten. Die Abstimmung der Datenschutzkonzepte einzelner Forschungsvorhaben hat danach auf der Grundlage des Leitfadens mit den jeweiligen betrieblichen bzw. behördlichen Datenschutzbeauftragten im Rahmen der gesetzlich geforderten Vorabkontrolle zu erfolgen. Die Stellungnahme der TMF nach dem oben beschriebenen Procedere ist dafür eine wesentliche Grundlage.

Eine Einbeziehung der zuständigen Datenschutz-Aufsichtsbehörde(n) ist grundsätzlich nicht notwendig, sie kommt aber in Betracht, wenn bei der

Konkretisierung des Leitfadens in Einzelfällen datenschutzrechtliche Fragestellungen auftreten, die inhaltlich nicht vom Leitfaden entschieden bzw. abgedeckt werden und von den Verantwortlichen vor Ort und ggf. der TMF nicht selbst beantwortet werden können oder als diskussionsbedürftig angesehen werden. In diesen Fällen kann sich der für das jeweilige Forschungsvorhaben zuständige betriebliche bzw. behördliche Datenschutzbeauftragte mit einem Beratungsersuchen, dem die Stellungnahme der TMF beigefügt werden sollte, an die zuständige Aufsichtsbehörde wenden.

Die für ein solches Beratungsersuchen zuständige Aufsichtsbehörde ist im Regelfall der Landesbeauftragte für den Datenschutz (LfD) des Bundeslandes, in dem die Zentrale oder Geschäftsstelle des für das Forschungsprojekt zuständigen Verbundes oder der durchführenden Einrichtung angesiedelt ist (vgl. Kap. 4.5). Im Falle eines bundeslandübergreifenden Forschungsprojekts übernimmt in der Regel diese Aufsichtsbehörde die Federführung für den weiteren Prozess. In diesem Falle sollen andere ggf. ebenfalls zuständige Aufsichtsbehörden von ihr informiert und in die Abstimmung einer gemeinsamen Stellungnahme eingebunden werden.

Eine solche Stellungnahme sollte von der betroffenen Forschungseinrichtung zusammen mit einer Aufstellung der ggf. noch erforderlichen Änderungen wiederum der Arbeitsgruppe Datenschutz vorgelegt werden, um so den Wissensfluss und -zuwachs in die TMF hinein aufrechtzuerhalten.

2.4 Gültigkeitsdauer und künftige Weiterentwicklung

Die erste Version der generischen Konzepte zum Datenschutz in der medizinischen Verbundforschung konnte nur die drängendsten datenschutzrechtlichen Probleme beim Aufbau langfristiger und vernetzter Forschungsinfrastrukturen lösen. Mit den 1999 gegründeten Kompetenznetzen in der Medizin wurde ein struktureller Umbau der Forschungslandschaft angestoßen, der mit einem zunehmenden Aufbau langfristiger zentralisierter Daten- und Probensammlungen einher ging und deren Nutzung zudem möglichst wenig durch eine enge Zweckbindung eingeschränkt werden sollte. In die jetzt vorgelegte revidierte Fassung ist viel Know-how aus der Anwendung der bisherigen Konzepte und der Beratung diverser und zum Teil sehr unterschiedlicher Projekte durch die Arbeitsgruppe Datenschutz der TMF eingeflossen. Vor diesem Hintergrund erscheint die Annahme begründet, dass diese Version den Bedürfnissen der medizinischen Forschungslandschaft für einige Zeit in der Zukunft gerecht werden könnte.

Eine Weiterentwicklung wird mittelfristig dennoch nötig sein: Die Forschungslandschaft und die gesetzlichen Rahmenbedingungen sind in Bewegung, und neue Erfahrungen mit der Anwendung werden auch in Zukunft gemacht. Insbesondere hat der erste Entwurf der Europäischen Kommission

für eine europäische Datenschutzgrundverordnung [6] deutlich gemacht, dass in den nächsten Jahren mit grundlegenden Umwälzungen des Datenschutzrechts mit Konsequenzen auch für nationale Regelungen zu rechnen ist. Daher wird es mit Sicherheit weitere Revisionen geben müssen, die wiederum die in den konkreten Projekten aufgetretenen und zurückgemeldeten Probleme aufgreifen werden. Auch in Zukunft wird daher der rege Informationsaustausch über den angewandten Datenschutz in der medizinischen Forschung in der Arbeitsgruppe Datenschutz der TMF und die enge Rückkopplung von Erfahrungen mit der Anwendung generischer Datenschutzkonzepte eine unabdingbare Voraussetzung für die Weiterentwicklung sein. Diesen Aufgaben wird sich die TMF auch in Zukunft stellen.

3 Anwendungsszenarien

Datensammlungen in medizinischen Forschungsdatenbanken und Registern sowie Probensammlungen in Biomaterialbanken dienen

- der Etablierung neuer Diagnose- und Therapiemethoden oder -optionen,
- der Standardisierung und Optimierung der Behandlungsverfahren,
- der Hypothesenbildung als Basis für kontrollierte klinische und epidemiologische Studien (Data Mining),
- der Analyse der molekulargenetischen Ursachen einer Krankheit und der Krankheitsmechanismen,
- der Identifizierung geeigneter Vorsorgemaßnahmen,
- der Evaluation der Leistungsfähigkeit des Versorgungssystems,
- der Erforschung der psychosozialen Folgen einer Erkrankung,
- der Rekrutierung geeigneter Patienten für klinische Therapiestudien,
- der Fallsuche für epidemiologische Studien oder
- der beschreibenden und analytischen Epidemiologie.

Diese Aufgabenstellungen werden in verschiedenen Kategorien medizinischer Forschung bearbeitet:

- Grundlagenforschung im Labor, die mit Biomaterialien und eventuell deren klinischen Begleitdaten („Annotation") arbeitet und dabei auch genetische Daten erzeugt.
- Klinische Studien, die der Prüfung neuer Diagnose- und Therapieverfahren direkt am Patienten dienen. Besonders bei seltenen Erkrankun-

gen oder großer Variabilität in den Krankheitsphänomenen müssen diese oft als „multizentrische" Studien aufgesetzt werden, um genügend viele Fälle für statistisch belastbare Aussagen zusammen zu bekommen.
- Epidemiologische Studien, die Krankheitsursachen und -trends im Bevölkerungsbezug erkunden oder die Langzeiteffekte therapeutischer Maßnahmen untersuchen.

Für alle diese Forschungsaufgaben sind genügende Fallzahlen oft nur durch Kooperation und Vernetzung zu erreichen; oft sind Langzeitspeicherung und -auswertung von Daten notwendig. In aller Regel werden Daten benötigt, die direkt bei der Versorgung von Kranken entstehen und daher einen stetigen Datenfluss aus der Versorgung in die Forschung erfordern. Die medizinische Forschung wird zunehmend in Forschungsverbünden zusammengefasst, die meistens krankheitsspezifisch orientiert sind und die Kooperation verschiedener Forschungsprojekte zum Ziel haben („horizontale Vernetzung") sowie den Daten- und Informationsfluss zwischen Versorgung und Forschung verbessern sollen („vertikale Vernetzung"), wie in Abbildung 3 illustriert.

In den folgenden Abschnitten dieses Kapitels werden die Abläufe in der medizinischen Forschung und ihr Nutzen für die betroffenen Patienten zunächst an zwei Fallbeispielen illustriert; daraus werden allgemeine Beschreibungen grundlegender Prozesse, insbesondere im Hinblick auf die Datenverarbeitung,

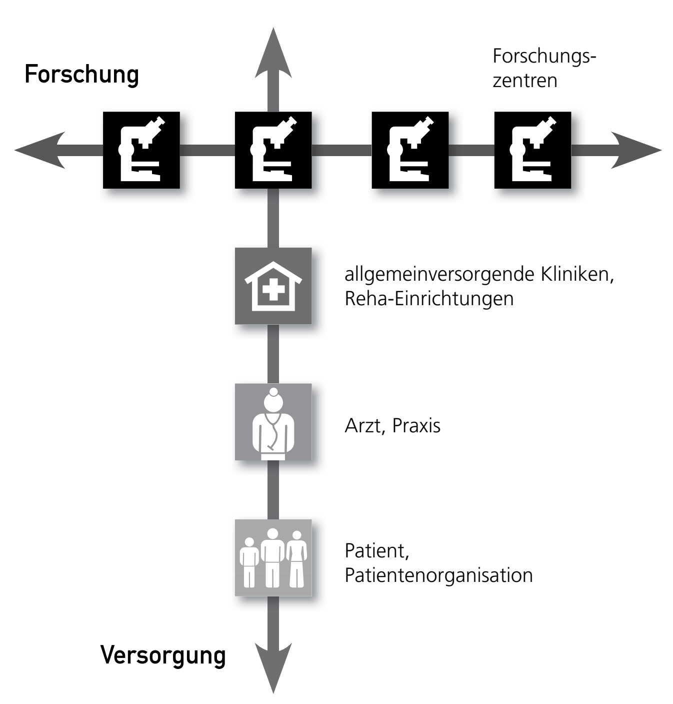


Abb. 3 Horizontale und vertikale Vernetzung in einem Forschungsverbund

abgeleitet. Danach folgt ein Ansatz zu einer formalen Spezifikation der Prozesse in Form von „Use Cases“; diese Spezifikation selbst wird wegen ihres Umfangs und ihres formalen Stils als Anhang inklusive umfangreichem Begleitmaterial online zur Verfügung gestellt[4].

3.1 Fallbeispiele

Die beiden folgenden Fallbeispiele sind bezüglich der vorgestellten Patienten und der Zukunftserwartungen fiktiv, beschreiben aber die Abläufe in typischen Projekten der medizinischen Verbundforschung realistisch.

3.1.1 „Kleine Petra“[5]

Bei der einjährigen Petra wird in der Mühlbach-Klinik in Saulheim ein Nierentumor (Wilms-Tumor, Nephroblastom) diagnostiziert. Die Mühlbach-Klinik arbeitet im Kompetenznetz Pädiatrische Onkologie und Hämatologie (KPOH) mit.

Mit dem KPOH ist das Deutsche Kinderkrebsregister (vgl. Kap. 5.3) assoziiert. Hier werden Daten über einen langen Zeitraum akkumuliert und u.a. für Spätfolgestudien genutzt. Außerdem sind mit dem KPOH eine Reihe multizentrischer klinischer Studien (vgl. Kap. 5.2) zu verschiedenen Therapiemethoden assoziiert, z.B. die Nephroblastomstudie SIOP2001, die u.a. klären soll, ob die postoperative Behandlung mit zusätzlicher Gabe des Zytostatikums Doxorubicin bei Patienten mit einem lokalen Stadium II oder III bei intermediärer Malignität für einen maximalen Therapieerfolg notwendig ist. Darüber hinaus sammelt das KPOH Tumorgewebe (vgl. Kap. 5.4), um dieses genetisch zu analysieren und u.a. mögliche Gründe für die Disposition zu einem Wilms-Tumor und prognostische Faktoren für individuell verschiedenes Ansprechen auf die Therapie zu finden.

Der behandelnde Arzt erläutert den Eltern die Auswirkungen eines Wilms-Tumors, Sinn und Abläufe des KPOH und des Krebsregisters sowie die möglichen Erfolgsaussichten und Risiken bestehender und neuer, zu evaluierender Therapieoptionen. Der behandelnde Arzt fragt dann die Eltern

- ob sie der Aufnahme von Petra in das Kinderkrebsregister zustimmen,
- ob sie der Teilnahme von Petra an der Nephroblastomstudie zustimmen sowie
- ob sie der Aufbewahrung von Gewebe und Proben auch für künftige Analysen zustimmen.

4 Alle Anhänge siehe unter http://www.tmf-ev.de/datenschutz-leitfaden
5 Diese fiktive Geschichte ist eine Überarbeitung einer von K. Pommerening und N. Graf für das Kompetenznetz Pädiatrische Onkologie und Hämatologie entworfenen Version.

Die Eltern stimmen alledem zu, weil sie wissen, dass neue Therapieoptionen aufgrund der notwendigen systematischen Evaluation zunächst nur im Rahmen von Forschungsprojekten zur Anwendung kommen können. Sie vertrauen auf eine sorgfältige und qualitätsgesicherte Behandlung und Betreuung im Rahmen des Forschungsnetzes. Petra wird an die Studienzentrale der Nephroblastomstudie und gleichzeitig an das Kinderkrebsregister gemeldet.

Ein Kernspin-Tomogramm wird zum Referenzradiologen geschickt. Der Referenzradiologie und die Studienleitung teilen den Befund der referenzradiologischen Beurteilung der Mühlbach-Klinik in einem gemeinsamen Schreiben mit. In diesem Schreiben wird zu folgenden Punkten Stellung bezogen:

- Die durchgeführte Diagnostik ist ausreichend, um eine sichere Diagnose zu stellen, oder sie muss durch bestimmte aufgeführte Untersuchungen ergänzt werden.
- Die Therapie der Patientin kann entsprechend dem Studienprotokoll beginnen oder muss abgeändert werden.

Nach präoperativer Behandlung wird Petra operiert und natives Tumormaterial zu wissenschaftlichen Untersuchungen zusammen mit einer Blutprobe an die Biomaterialbank für Nephroblastome des KPOH geschickt. Gewebeschnitte werden über den lokalen Pathologen zum Referenzpathologen des KPOH zur Sicherung der exakten Diagnose weitergeleitet.

Der Studienleiter, der der führende deutsche Experte für Wilms-Tumoren ist, teilt Petra aufgrund der exakten Diagnose und einer Randomisierung einem Studienarm mit festgelegtem Therapieablauf zu. Falls eine Strahlentherapie erforderlich ist, wird der Referenzstrahlentherapeut der Studie mit Hilfe der in der Studienzentrale vorliegenden Daten einen Bestrahlungsplan für Petra erstellen. Eventuell müssen weitere Bilder und Daten von der Mühlbach-Klinik angefordert werden.

Während der Durchführung steht der Studienleiter jederzeit zur Konsultation für die behandelnde Klinik zur Verfügung. Therapieverlaufsdaten werden regelmäßig an die zentrale Studiendatenbank, außerdem in stark reduzierter Form an das Kinderkrebsregister übermittelt. Informationen über auftretende ernste Nebenwirkungen (so genannte SUSARs) werden von der Studienzentrale allen beteiligten Studienkliniken kurzfristig weitergeleitet.

Nach fünf Monaten mit Chemotherapie und Operation wird Petra als geheilt entlassen. Nach weiteren zwei Jahren wird Petra zu einer Nachuntersuchung eingeladen. Petra ist rezidivfrei.

Ein Jahr später wird die Studie abgeschlossen und ausgewertet: Kinder mit reduzierter Zytostatikagabe wurden genauso oft geheilt und hatten signifikant weniger unter Nebenwirkungen zu leiden als die Vergleichsgruppe.

In ihrem achtzehnten Lebensjahr wird Petra vom Kinderkrebsregister angeschrieben und um ihre Zustimmung zur weiteren Aufbewahrung ihrer Daten

gebeten. Gleichzeitig wird sie zu einer Spätfolgenstudie eingeladen und dabei zu ihrem Gesundheitszustand befragt. Für eine weitere Studie zur Lebensqualität von ehemaligen Wilms-Tumor-Patienten gibt Petra die Auskunft, dass sie trotz einer fehlenden Niere ein normales Leben führt.

Eine zwischenzeitlich gefundene neue Analysemethode – die zur Zeit der Gewebeeinlagerung noch nicht bekannt war – hat ergeben, dass Petras Risiko, einen weiteren Wilms-Tumor – etwa an der zweiten Niere – zu bekommen, sehr gering ist. Ebenso kann ihr mitgeteilt werden, dass für eigene Kinder kein erhöhtes Risiko besteht, an einem Nephroblastom zu erkranken. Da sie einer Rückmeldung solcher Analyseergebnisse zugestimmt hatte, kann sie diesen Befund mit Erleichterung zur Kenntnis nehmen.

3.1.2 „Kleiner Timo"

Als Timo geboren wurde, fiel sofort auf, dass seine Haut an mehreren Stellen verletzt war. Der hinzugezogene Dermatologe stellte die Verdachtsdiagnose einer Epidermolysis bullosa (EB). Es handelt sich um eine seltene erbliche Hauterkrankung, bei der aufgrund verschiedener Gendefekte der Zusammenhalt zwischen den Schichten der Haut gestört ist. Schon geringe Traumata können dann zur Blasenbildung von Haut und Schleimhäuten führen, denen je nach Typ der Erkrankung weitere Komplikationen folgen können. Eine ursächliche Therapie ist noch nicht bekannt, nur eine symptomatische Behandlung ist bisher möglich.

Aufgrund ihres seltenen Vorkommens (ca. 1 Fall pro 100.000 Geburten) kann die Erkrankung nur sehr schwer erforscht werden: Einzelne Zentren erreichen keine ausreichenden Fallzahlen für statistisch signifikante Auswertungen. Aus diesem Grund wurden für eine Reihe von seltenen Erkrankungen Forschungsnetze gegründet, in denen ihre Behandlung und Erforschung einrichtungsübergreifend und überregional durchgeführt wird (vgl. Kap. 6.7.5).

Timo wird an ein spezialisiertes Zentrum innerhalb des Netzwerks Epidermolysis bullosa überwiesen. Dort kann die Diagnose mit Hilfe einer Biopsie gesichert werden. Zu diesem Zeitpunkt werden Timos Eltern über das Netzwerk informiert. Im Rahmen eines Aufklärungsgesprächs wird ausführlich auf die Möglichkeiten zur regelmäßigen Beobachtung und Behandlung der Erkrankung innerhalb des Netzwerks eingegangen. Außerdem wird diskutiert, wie durch die Zusammenstellung und Auswertung der Beobachtungen und Untersuchungen an Timo und anderen Betroffenen das Wissen über die Erkrankung vermehrt und die Chancen, eine ursächliche Therapie zu finden, verbessert werden können. Hierbei wird auch über die Erhebung von Daten und ihre Weitergabe und Verarbeitung in pseudonymisierter Form innerhalb des Netzwerks gesprochen. Die Pseudonymisierung ermöglicht hierbei sowohl einen effektiven Schutz der persönlichen Daten als auch die Chance einer späteren Kontaktierung des Patienten, falls aufgrund relevanter Forschungsergebnisse

ein berechtigtes Interesse dazu besteht. Vor dem Hintergrund, dass es sich bei der Epidermolysis bullosa um eine seltene, stigmatisierende Erkrankung handelt, wird ebenfalls darauf eingegangen, dass das Risiko einer ungewollten Reidentifikation eines Patienten nicht völlig ausgeschlossen werden kann. Für Timos Eltern überwiegt jedoch die Möglichkeit, von neuen Behandlungsoptionen zu profitieren, die angesprochenen Risiken, so dass sie für Timo die Einwilligung zur Teilnahme am Netz geben. Zudem wollen sie die Forschung in diesem für sie persönlich wichtigen Bereich der Medizin unterstützen.

Im Rahmen der Aufnahmevisite werden standardisierte Untersuchungsbefunde erhoben und Timos Eltern zu Symptomen und zum Befinden befragt. Die Daten werden anschließend in die Erhebungssoftware des Netzwerks eingetragen. Da das Netzwerk EB versorgungsnah arbeitet, werden die Erhebungsbögen von den behandelnden Ärzten selbst oder von beauftragten Dokumentationsassistenten eingegeben (vgl. Kap. 5.1). Mit Hilfe der entnommenen Gewebeproben wird der exakte Subtyp der EB diagnostiziert und eine Mutationsanalyse zur Feststellung des ursächlichen Gendefekts durchgeführt. Die hierbei ermittelten Daten werden ebenfalls in der Erhebungssoftware gespeichert. Im Behandlungszusammenhang darf es nicht zu Verwechslungen kommen, daher wird an dieser Stelle nicht mit Pseudonymen, sondern mit den Namen und Geburtsdaten der Patienten (identifizierende Daten) gearbeitet. Um unerlaubte Zugriffe zu verhindern, werden die identifizierenden und die medizinischen Daten in getrennten Systemen an räumlich und organisatorisch verschiedenen Standorten des Netzwerks gespeichert und erst auf dem Rechner des behandelnden Arztes zusammengeführt.

Timos weitere Behandlung wird heimatnah fortgesetzt, wobei auf Fachinformationen und Therapiehinweise des Netzwerks EB zurückgegriffen werden kann. Ärzte des Netzwerks stehen im Rahmen des Behandlungszusammenhangs für Rückfragen der Ärzte vor Ort zur Verfügung. In regelmäßigen Abständen stellen sich Timo und seine Eltern wieder in einer klinischen Einrichtung des Netzwerks für eine Follow-up-Untersuchung vor. Hierbei kann der klinische Verlauf mit Hilfe der bereits erhobenen Daten verfolgt und die Datenbank des Netzwerks um die aktuellen Befunde ergänzt werden.

Ein Blick in die Zukunft: Timo ist inzwischen erwachsen. Neben der Tatsache, dass er nur eine leichte Form der Erkrankung hat, trägt die Betreuung im Netzwerk wesentlich zu seiner Lebensqualität bei. Da er jetzt selbst über die Teilnahme an der Studie entscheiden muss, wird ein erneutes Aufklärungsgespräch mit ihm geführt und er gibt seine Einwilligung. In der Zwischenzeit wurden mit Hilfe der gesammelten Daten und Gewebeproben (vgl. Kap. 5.4) erste Ansätze für eine ursächliche Therapie entdeckt, die aber noch weiter untersucht werden müssen. Timo hofft, dass er hierzu einen Beitrag leisten und vielleicht selbst einmal im Rahmen einer Therapiestudie davon profitieren kann. Er willigt deshalb auch ein, für zukünftig geplante Studien kontaktiert zu werden (vgl. Kap. 3.2.4.5).

3.1.3 Allgemeine Aspekte

Einige allgemeine Aspekte medizinischer Forschung werden aus diesen Fallbeispielen deutlich:

- Krankenversorgung und medizinische Forschung sind eng verzahnt: Für beide Bereiche werden gleiche Daten benötigt; Studienleiter wirken bei Studien oft konsiliarisch an der Behandlung mit, ebenso andere Experten im Netz, z.B. im Rahmen der Referenzdiagnostik, die eine unmittelbare Auswirkung auf die Behandlung haben kann.
- Forschungsverbünde können viele Komponenten und kooperierende Teilprojekte haben.
- Überregionale oder internationale Kooperationen sind notwendig, insbesondere um bei seltenen Erkrankungen ausreichende Fallzahlen zusammen zu bekommen, aber auch um das Wissen hoch spezialisierter Experten einzubinden.
- Langfristige Datenspeicherung und Probenaufbewahrung sind notwendige Grundlage für den medizinischen Fortschritt; viele Forschungsprojekte wären sonst nicht durchführbar.
- Medizinische Forschung nützt manchmal dem Patienten selbst, oft aber erst künftigen Patientengenerationen. Trotz dieses Wissens ist die Motivation der Patienten zur Teilnahme an Forschungsprojekten sehr hoch; sie möchten natürlich jede Chance eines möglichen persönlichen Nutzens wahrnehmen, haben aber in den allermeisten Fällen auch den Wunsch, dass aus ihrem Fall Hilfe für künftige Leidensgenossen entstehen soll [7].

3.2 Prozesse und Abläufe im medizinischen Forschungsverbund

Die Komponenten in einem medizinischen Forschungsverbund, deren Rolle in den Fallbeispielen ansatzweise illustriert wurde, sind auf verschiedenartige medizinische Forschungsprojekte zugeschnitten und spiegeln deren Besonderheiten:

- Kontrollierte klinische Studie, die eine konkrete Zielsetzung in Gestalt der Prüfung einer Hypothese hat. Solche Studien sind häufig durch AMG (und MPG) sowie GCP-Richtlinien reguliert [8].
- Klinisches Register, z.B. Krebsregister, das der langfristigen lokalen oder regionalen Dokumentation von Fällen einer bestimmten Erkrankung dient.
- Klinisches „Datawarehouse“, in dem Patientendaten eines Krankenhauses in aufbereiteter Form langfristig für Auswertungen, künftige Forschungsprojekte und „Rekrutierung“ geeigneter Fälle aufbewahrt werden.
- Epidemiologisches Register, das langfristig und bevölkerungsbezogen angelegt ist.
- Kohorte, die zur Langzeitbeobachtung einer festen Teilmenge der Bevölkerung eingerichtet wird.

- Klinische Datenbank als einrichtungsübergreifendes Register zur Erforschung seltener oder chronischer Erkrankungen, bei denen oft zunächst nur systematische Datensammlungen im Rahmen von Beobachtungsstudien und Heilversuchen möglich sind; manchmal ergänzt um einen ständigen Erfahrungsaustausch von Experten zu konkreten Patientendaten.
- Bilddatenbank, in der medizinische Bilder gesammelt, aufbereitet, durch Daten des Patienten ergänzt und in geeigneter Form als Referenzmaterial für Versorgung, Forschung und Lehre zur Verfügung gestellt werden.
- Biobank, in der Rohmaterial für die klinische und translationale Forschung, sowie die genetische Epidemiologie gesammelt wird.

In einem krankheitsbezogenen Forschungsverbund kooperieren solche verschiedenen Projekte, Studien und Register oft in größerer Anzahl. Selbstverständlich werden solche Projekte sehr häufig auch als eigenständige Vorhaben ohne Einbindung in ein Netzwerk durchgeführt.

Eine Beschreibung der dabei ablaufenden Prozesse ist die Grundlage zum Entwurf einer IT-Architektur und zur Analyse der Datenverarbeitungserfordernisse unter dem Gesichtspunkt datenschutzrechtlicher Anforderungen. Im Folgenden werden die wichtigsten direkt aus der Zweckbestimmung des Forschungsprojekts oder -verbunds sich ergebenden notwendigen Abläufe, ihr jeweiliger Zweck und ihre Grobstruktur beschrieben. Verfeinerungen, insbesondere datenschutzrechtlicher Natur, werden später in den unterschiedlichen Anwendungsbereichen hieraus abgeleitet. Ein Ansatz zu einer stärker formalisierten und detaillierteren Beschreibung wird im folgenden Kapitel 3.3 vorgestellt; diese Formalisierung erleichtert auch eine Vollständigkeitsprüfung und ist eine wichtige Hilfe bei der Implementierung in einem IT-System.

Die Prozessabläufe bei der Datengewinnung (s. Kap. 3.2.1), beim Datenmanagement (s. Kap. 3.2.2) und bei der Datenauswertung (s. Kap. 3.2.3.5) werden in Abbildung 4 grob skizziert.

3.2.1 Datengewinnung

3.2.1.1 Patienten aufnehmen

Zweck und Anwendungsbereich: Daten oder Proben eines Patienten, der für ein Forschungsprojekt oder einen Forschungsverbund geeignet erscheint, sollen für die entsprechenden Daten- oder Probenbanken (Studie, Register, Kohorte, Datenbank, Biobank) in dem Umfang bereitgestellt werden, der dem jeweiligen Datenmodell entspricht. Voraussetzung ist eine informierte Einwilligung des Betroffenen (s. Kap. 3.2.3.1).

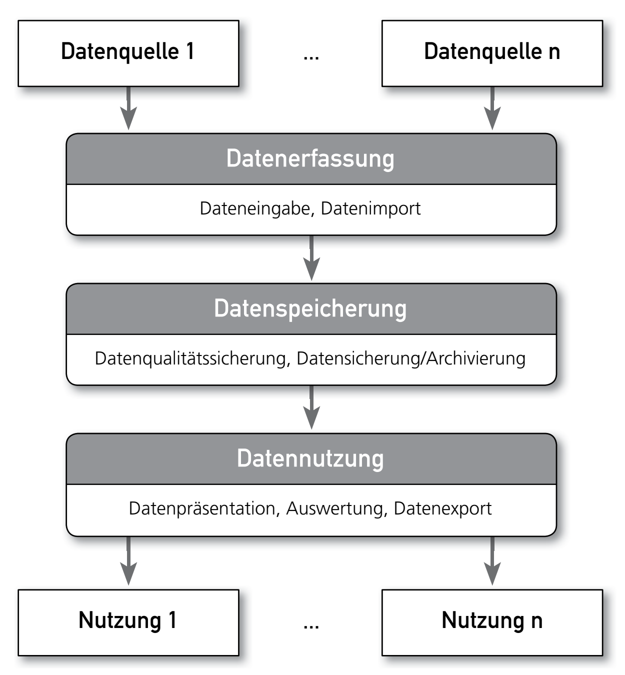


Abb. 4 Komponenten des Datenmanagements in einem Forschungsprojekt oder -verbund. Die Prozessierung von Proben verläuft analog.

Prozessablauf: Der Patient erscheint zur Behandlung, wird als geeignet für die Teilnahme am Forschungsverbund (bzw. einem Forschungsprojekt oder einer Komponente des Forschungsverbunds) eingeschätzt. Es findet ein Aufklärungsgespräch statt, die Einwilligung des Patienten wird eingeholt (s. Kap. 3.2.3.1). In der Regel wird für das Projekt eine zusätzliche Referenzbefundung veranlasst. Handelt es sich um eine klinische Studie (s. Kap. 3.2.5.1) oder eine Biobank (s. Kap. 3.2.5.2), sind evtl. weitere Schritte nötig. Kontaktdaten des Patienten werden für das Kontaktmanagement (s. Kap. 3.2.3) erfasst. In der Regel werden auch wichtige medizinische Daten in einem „Ersterhebungsbogen" an die Datenbank des Projekts oder die passenden Datenbanken des Forschungsverbunds übermittelt.

3.2.1.2 (Gesunden) Probanden aufnehmen

Zweck und Anwendungsbereich: Für viele Typen von Studien werden gesunde Personen als Vergleichspersonen zur Gewinnung oder Prüfung von Hypothesen benötigt. So wird etwa in einer epidemiologischen Fall-Kontroll-Studie die Frage verfolgt, ob eine vorhandene Gruppe von Erkrankten einer bestimmten Exposition in anderem Ausmaß ausgesetzt war als eine Vergleichsgruppe von Gesunden. Anwendungsbereiche dieses Prozesses sind epidemiologische Register, Kohorten und Biobanken.

Prozessablauf: Im Gegensatz zu Patienten müssen gesunde Probanden erst gefunden werden; wie das geschieht, ist projektspezifisch. Dann laufen Aufklärung, Einwilligung, Kontaktdatenerfassung und Ersterhebung wie bei Patienten ab. Ein Behandlungszusammenhang entsteht für gesunde Probanden nur, wenn zur Datengewinnung medizinische Diagnostik notwendig ist oder wenn Proben abgenommen werden, nicht aber bei einer bloßen Befragung oder Datenerhebung.

3.2.1.3 Daten erheben

Zweck und Anwendungsbereich: Es werden die für das jeweilige Projekt (Studie, Register, Kohorte, Biobank) oder den Forschungsverbund gemäß dem Datenmodell nötigen Daten erhoben und zur Speicherung an die entsprechende(n) Datenbank(en) übermittelt.

Prozessablauf: Nach der Aufnahme in das Forschungsprojekt oder den Forschungsverbund (s. Kap. 3.2.1.2) erfolgt die primäre Datenerhebung (für Studie, Register, Kohorte, Biobank). Bereits vor der Aufnahme gewonnene Daten aus dem Behandlungszusammenhang werden für das Projekt oder den Forschungsverbund bereitgestellt. Zusätzliche Daten werden durch projektspezifische Prozeduren, z.B. Referenzbefundung oder Befragung gewonnen. Die Daten werden entweder über ein EDC-System oder eine Export-Schnittstelle an die entsprechende Datenbank übermittelt. Analog wird bei Follow-up-Daten (z.B. bei späterer Weiterbehandlung oder Nachbefragung) verfahren. Für Besonderheiten bei Biobanken siehe Kapitel 3.2.5.2.

3.2.1.4 Daten mit externen Quellen abgleichen

Zweck und Anwendungsbereich: Für manche Projekte (z.B. epidemiologisches Register, Kohorte, evtl. klinisches Register) ist es wichtig, auch Daten aus anderen Quellen heranzuziehen, die sonst nicht zu gewinnen wären, beispielsweise Sterbedaten aus dem Einwohnermeldeamt für ein epidemiologisches Register, um Sterblichkeitsraten und Überlebenszeiten analysieren zu können. Der umgekehrte Fall, dass Daten des Forschungsverbunds für ein anderes Projekt zum Abgleich herangezogen werden, wird unter dem Stichwort „Datennutzung“ in Kapitel 3.2.4.7 behandelt.

Prozessablauf: Es wird eine Anfrage an die externe Datenquelle gestellt und von dieser (nach Überprüfung der Rechtslage) eine Exportdatei mit den benötigten Daten zurückgeliefert. In der Regel werden die Daten für den Abgleich nur pseudonymisiert bereitgestellt, eventuell wird ein Datentreuhänder eingeschaltet.

3.2.2 Datenmanagement

Für das Datenmanagement ist in der Regel gesondert geschultes Personal notwendig, das hier in der Rolle „Datenmanager“ zusammengefasst wird. Es handelt sich dabei meist um Informatiker, Biostatistiker oder medizinische Dokumentare. Der Datenmanager betreut eine oder mehrere Datenbanken auf der inhaltlichen Ebene; die technische Betreuung ist eine gesonderte Aufgabe, die nicht zum eigentlichen Datenmanagement gehört, allerdings bei kleineren Projekten oft in Personalunion bearbeitet wird. Das Datenmanagement schließt oft auch Auswertungen ein.

3.2.2.1 Rechte vergeben

Zweck und Anwendungsbereich: Der Umgang mit medizinischen Daten in einem Forschungsprojekt oder -verbund erfordert eine sorgfältige Regelung der Zugriffsrechte, die durch Rollenzuweisungen strukturiert wird und dem „Need-to-know“-Prinzip folgt (s.a. Kap. 6.2). Grundlage dafür sind die in einer Policy festgeschriebenen Regeln des Forschungsverbunds.

Prozessablauf: Zugriffsrechte sind an Personen oder Rollen gebunden; für die konkrete Zuweisung ist der Datenmanager der jeweiligen Datenbank verantwortlich. In einigen Fällen, z.B. bei der Mit- oder Weiterbehandlung ist es auch sinnvoll, den Patienten aktiv einzubeziehen. Für die Rechte- und Rollenverwaltung werden geeignete Werkzeuge genutzt. Dabei wird auch überprüft, ob die vergebenen Rechte mit der Richtlinie („Policy“) des Forschungsprojektes oder Forschungsverbunds konsistent sind.

3.2.2.2 Datenqualität sichern

Zweck und Anwendungsbereich: Daten, die an eine Datenbank übermittelt werden, sind oft fehlerbehaftet, unvollständig oder anderweitig nicht unmittelbar für den intendierten Zweck geeignet; beispielsweise können Eingabefehler auftreten, oder die Daten stammen aus einem anderen Kontext mit anderer Zielsetzung (z.B. aus dem Behandlungskontext, wo eine Nebendiagnose mangels Abrechnungsrelevanz nicht erfasst wurde) oder mit anderem Datenmodell (z.B. mit anderen Klassengrenzen bei der Diskretisierung von Merkmalen). Die Datenqualitätssicherung sorgt dafür, dass die Daten für das jeweilige Forschungsprojekt so aufbereitet werden, dass sie die notwendigen Anforderungen an Korrektheit und Vollständigkeit erfüllen.

Prozessablauf: Datenüberprüfung schon bei Eingabe, z.B. auf Vollständigkeit und Plausibilität, soweit möglich im EDC-System automatisiert. Oft, besonders bei klinischen Studien, wird für die Datenerfassung auch besonders geschultes Personal („Studienassistenten“, „Study Nurses“) eingesetzt. Bei Fehlern oder Zweifelsfällen erfolgt eine Rückfrage an die Datenquelle und ggf. eine Korrektur der Daten. In besonderen Fällen, vor allem bei klinischen Stu-

dien (s. Kap. 3.2.5.1) ist auch ein Rückgriff des Datenmanagers auf die Quelldaten zur Verifikation notwendig. Eine detailliertere Beschreibung folgt in Kapitel 6.8. Zur Datenqualitätssicherung gehört auch das Monitoring (s. Kap. 6.8.3.2).

3.2.2.3 Audit durchführen oder unterstützen

Zweck und Anwendungsbereich: Ein Audit-Verfahren dient der Überprüfung, ob die in den verbindlichen Verfahrensbeschreibungen („SOPs“) festgelegten Abläufe eingehalten werden. Ein solches Verfahren wird in der Regel von einem externen (vertrauenswürdigen) Auditor durchgeführt.

Prozessablauf: Ein Audit-Verfahren umfasst den Vor-Ort-Besuch bei allen am Forschungsprojekt oder -verbund beteiligten Stellen und dort jeweils die Kontrolle aller Verfahrensdokumentationen und Abläufe; Einblicke in die Daten müssen, soweit notwendig, gewährt werden. Einblick in Identitätsdaten ist dabei in der Regel nicht notwendig (s.a. Kap. 6.8.2.5).

3.2.2.4 Unerwartete Ereignisse managen

Zweck und Anwendungsbereich: Unerwartete Ereignisse von medizinischer Relevanz können in jedem klinischen Forschungsprojekt auftreten und führen zu bestimmten Kommunikationsanforderungen. Besonders gesetzlich geregelt sind diese im AMG für klinische Studien mit einem besonderen, pharmakologisch begründeten Risikopotenzial für die Probanden. Neben der behandlungsseitigen, klinischen Dokumentation solcher Ereignisse ist somit auch eine Dokumentation im Zusammenhang mit dem Forschungsprojekt notwendig.

Prozessablauf: Unerwartete Ereignisse sind von den behandelnden Ärzten zu dokumentieren und ggf. an zuständige Forscher zu kommunizieren. Dabei ist im Regelfall eine Einstufung des Schweregrads des Ereignisses und der Wahrscheinlichkeit eines Zusammenhangs mit der im Rahmen des Forschungsvorhabens ggf. durchgeführten Intervention vorzunehmen. Schwerwiegende unerwartete Ereignisse (SAEs) sind in Studien nach dem Arzneimittelrecht vom Prüfer an den Sponsor zu melden. Abhängig von dem Schweregrad eines Ereignisses sind ggf. auch Ethikkommissionen und zuständige Behörden zu informieren.

3.2.2.5 Daten zwischen den Modulen eines Forschungsverbunds übermitteln

Zweck und Anwendungsbereich: Ein Forschungsverbund besitzt meist mehrere Datenbanken mit unterschiedlicher Zweckbestimmung, z.B. ein klinisches und ein epidemiologisches Register, in denen dennoch die Daten zu den gleichen Patienten vorgehalten werden können. Um mehrfache Datenerhebung zu vermeiden und die Datenbestände konsistent zu halten, sind Datenabgleiche zwischen diesen Datenbanken notwendig (genauer beschrieben in Kap. 6.3 bis 6.5).

Prozessablauf: Es kann sich um einen kontinuierlichen Datenabgleich handeln, der zeitnah mit der Entstehung neuer Daten durchgeführt wird, oder um einen in regelmäßigen Abständen, dann meist manuell, angestoßenen Prozess. Festlegungen aus der Einwilligungserklärung sind hierbei zu beachten, etwa wenn ein Patient nicht an allen passenden Projekten des Forschungsverbunds teilnehmen will.

3.2.2.6 Daten und Dokumente archivieren

Zweck und Anwendungsbereich: Die Nachprüfbarkeit von Forschungsergebnissen erfordert, dass die verwendeten Daten für unabhängige Verifikationen auch nach Abschluss des Projekts vorgehalten werden.

Prozessablauf: Die zu archivierenden Daten werden in der Regel anonymisiert oder pseudonymisiert und dann in einen getrennten Datenbestand überführt. Falls die Wahrung der Rechtsverbindlichkeit notwendig ist (wie bei klinischen Studien), können Verfahren mit qualifizierter elektronischer Signatur eingesetzt werden. Bei Einhaltung anerkannter Qualitätsstandards und einer entsprechend vollständigen Verfahrensdokumentation können alternativ aber auch andere Verfahren zum Einsatz kommen. Nach Überführung in den Archiv-Datenbestand werden die Daten aus der ursprünglichen Datenbank gelöscht. Ausführliche Hinweise zu diesem Thema finden sich in einem im Auftrag der TMF erstellten Rechtsgutachten [9; 10].

3.2.3 Kontakt mit Betroffenen

Wesentliche Prozessabläufe, die den Kontakt zwischen Patienten (oder Probanden) und dem Forschungsverbund betreffen, werden in Abbildung 5 illustriert.

Gründe für die Kontaktierung von Patienten (oder Probanden) über den Erstkontakt hinaus können sein:

- eine Erinnerung an die notwendige Weiterbehandlung/Wiedereinbestellung im Behandlungszusammenhang,
- die Rückmeldung von Befunden aus einem Forschungsprojekt (z.B. genetische Disposition) im Rahmen des in der Einwilligungserklärung abgebildeten Rechts auf Wissen oder Nichtwissen,
- Nacherhebungen, Befragungen,
- oder auch die Rekrutierung für neue Projekte.

Im Normalfall ist der behandelnde Arzt für einen Patienten die Kontaktperson zum Forschungsprojekt oder -verbund; dieser kann im Laufe der Behandlung allerdings wechseln. In manchen Fällen ist auch ein direkter Kontakt zwischen Patient (oder Proband) und anderen Repräsentanten des Forschungsverbunds sinnvoll.

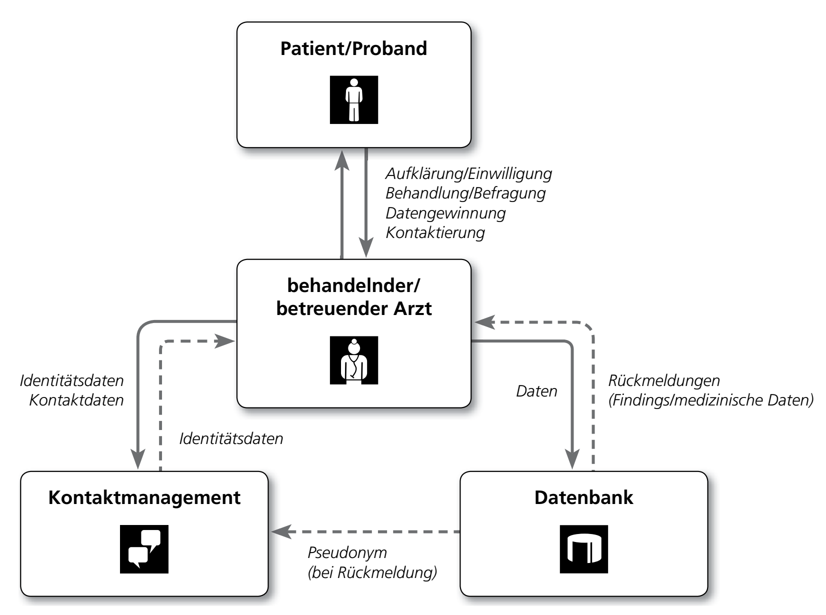


Abb. 5 Komponenten des Kontaktmanagements in einem Forschungsverbund

3.2.3.1 Probanden aufklären und Einwilligung einholen

Zweck und Anwendungsbereich: Medizinische Forschung mit personenbeziehbaren Daten erfordert im Regelfall eine informierte Einwilligung der Betroffenen. Diese muss vor der Aufnahme in ein Forschungsprojekt oder einen Forschungsverbund eingeholt werden.

Prozessablauf: Nach einem Aufklärungsgespräch, in dem alle Fragen des Probanden beantwortet werden, und einer nötigen Bedenkzeit, erfolgt eine schriftliche Einwilligung. Das unterschriebene Einwilligungsformular wird sicher aufbewahrt und der Umfang der Einwilligung im Kontaktmanagement gespeichert. In der Regel wird der Patient vom „Erstbehandler" durch diesen Prozess geführt, bei gesunden Probanden geschieht dies eventuell auch durch Forschungspersonal. Ausführliche Informationen zu diesem Prozess finden sich bei Harnischmacher et al. [5].

3.2.3.2 Kontaktdaten aktualisieren

Zweck und Anwendungsbereich: Aktuelle Kontaktdaten werden in einer nur dafür vorgesehenen Datenbank verwaltet. Diese ist als Teil des Identitätsmanagements für Patienten und Probanden anzusehen und wird in Kapitel 6.1 ausführlich behandelt.

Prozessablauf: Die wesentlichen Prozesse sind: Kontaktdaten erfassen, pflegen, ändern, löschen. Als Werkzeug dafür kann CRM-Software (Customer Relationship Management) geeignet sein.

3.2.3.3 Auskunft geben

Zweck und Anwendungsbereich: Betroffene haben das Recht auf Auskunft über die von ihnen gespeicherten personenbezogenen Daten. Zudem sind diese auf Verlangen der Betroffenen auch zu korrigieren (vgl. Kap. 4.4.1).

Prozessablauf: Der Betroffene wendet sich an seinen behandelnden Arzt als Kontaktperson zum Forschungsprojekt oder -verbund. Es muss auch möglich sein, den Forschungsverbund direkt zu kontaktieren, etwa über das Leitungsgremium oder einen Datenmanager. Bei dieser Kontaktperson meldet er sein Anliegen an. Ein geeigneter Rückmeldemechanismus teilt ihm die verlangte Auskunft oder den Vollzug der beantragten Aktion mit.

3.2.3.4 Ergebnisse mitteilen

Zweck und Anwendungsbereich: Wenn im Rahmen eines Forschungsvorhabens umfangreiche medizinische Daten gesammelt werden, kann deren Auswertung, manchmal auch nach Abschluss des Vorhabens, zu unerwarteten, für den Betroffenen direkt relevanten ärztlichen Beobachtungs- oder Untersuchungsergebnissen („Findings“) führen, über die ein Patient – im Rahmen der Festlegungen der Einwilligungserklärung – zu informieren ist.

Prozessablauf: Diese Rückmeldung wird in der Regel über den behandelnden Arzt gegeben. Hierzu wird letzterer durch den zuständigen Mitarbeiter des Forschungsprojekts gemäß den Regelungen des Forschungsverbunds benachrichtigt; er kontaktiert dann seinerseits den Patienten. In Ausnahmefällen kann auch eine direkte Rückmeldung vom Forschungsprojekt an den Patienten vorgesehen sein; hier wird der Betroffene mit Hilfe des Kontakt- oder Identitätsmanagements kontaktiert. Bei genetischen Befunden sind die Regelungen des Gendiagnostikgesetzes zu befolgen, insbesondere die Heranziehung eines humangenetisch qualifizierten Arztes.

3.2.3.5 Daten sperren, anonymisieren oder löschen

Zweck und Anwendungsbereich: Betroffene haben das Recht, ihre Einwilligung in die Verarbeitung, Speicherung und Nutzung personenbezogener Daten zu widerrufen. In diesem Falle sind die Daten zu sperren, zu anonymisieren oder auch zu löschen. Welche dieser Maßnahmen zu treffen ist, hängt von der Art des Widerrufs, dem konkreten Anwendungsfall und ggf. auch dem Umfang der gespeicherten medizinischen Daten ab.

Prozessablauf: Der Betroffene wendet sich an seinen behandelnden Arzt als Kontaktperson zum Forschungsprojekt oder -verbund. Es muss auch möglich sein, den Forschungsverbund direkt zu kontaktieren, etwa über das Leitungsgremium oder einen Datenmanager. Daraufhin ist durch das Datenmanagement die Sperrung, Anonymisierung oder Löschung der Daten vorzunehmen. Dabei

ist auf die korrekte Reihenfolge der Aktionen zu achten, so dass alle Datensätze über das zuletzt gültige Pseudonym angesprochen werden können und eine Rückmeldung zu allen Aktionen erfolgen kann. Die erfolgreiche Durchführung sollte dem Betroffenen zurückgemeldet werden. Dies erfordert, dass die Kontaktdaten erst ganz zum Schluss gelöscht werden dürfen.

3.2.4 Datennutzung

3.2.4.1 Referenzbefundung einbinden

Zweck und Anwendungsbereich: Qualitätssicherung der Diagnose durch externen Experten, meistens Radiologe oder Pathologe, Zuweisung zu Studienarmen bei klinischen Studien. Diese Referenzbefundung ist in der Regel behandlungsrelevant, findet aber gelegentlich auch erst nach dem Tode des Patienten statt und dient dann der Qualitätssicherung von Forschungsdaten.

Prozessablauf: Dem externen Experten wird das benötigte Material übermittelt (Proben, Gewebeschnitte) bzw. Zugriff auf die benötigten Daten gewährt (Röntgenbilder, mikroskopische Aufnahmen). Er meldet seinen Befund an das Forschungsprojekt, in der Regel auch an den behandelnden Arzt zurück. Nach Abschluss der Referenzbefundung wird übriges Biomaterial vernichtet oder in eine Biobank überführt und der Datenzugriff wieder gesperrt.

3.2.4.2 Expertenforum organisieren

Zweck und Anwendungsbereich: In einigen medizinischen Forschungsverbünden ist die Einrichtung von Expertenforen sinnvoll, in denen ausgewählte Experten medizinische Aspekte von Erkrankungsfällen diskutieren. Dieses Szenario ist vor allem bei seltenen Erkrankungen von Bedeutung, aber auch in anderen Verbünden notwendig, wenn es um schwierige Diagnosen und Therapieempfehlungen geht, so z.B. als Erfahrungsaustausch bei Beobachtungsstudien und Heilversuchen.

Ein solches Forum dient der fallbezogenen Diskussion zu einer Erkrankung. Konkrete Fragen zu Diagnose oder Therapie können gestellt werden; es sollen aber auch spontane Beiträge möglich sein, die Hypothesen oder Ideen formulieren.

Teilnehmer des Forums sind namentlich benannte Experten, die persönlich zum Forum zugelassen werden. Diese können auch im Ausland ansässig sein. Die Liste der Experten sollte dem betroffenen Patienten, idealerweise sogar öffentlich zugänglich sein. In der Patientenaufklärung sollte darauf hingewiesen werden.

Prozessablauf: Datenspeicherung in einer klinischen Datenbank (behandlungsbezogene Patientendatenbank). Online-Zugang für die Experten, befristet für die Dauer der Diskussion, etwa 2 bis 4 Wochen; danach wird der Zugang zum

jeweiligen Fall wieder gesperrt. Ein Zugriff auf Identitätsdaten ist hierbei nicht notwendig.

3.2.4.3 Daten an eine Referenzdatenbank weitergeben

Zweck und Anwendungsbereich: Daten zu einem Krankheitsfall (Kasuistik, Bildmaterial, Analysenergebnisse) können als Referenzmaterial für ähnlich gelagerte Fälle verwendet werden; das kann gerade im Rahmen von Beobachtungsstudien und Heilversuchen sowie bei seltenen Erkrankungen relevant sein. Referenzmaterial ist auch im Rahmen von Lehre und Ausbildung nötig.

Prozessablauf: Qualitätsgesicherte anonymisierte Daten werden über eine Datenbank für Berechtigte angeboten. Hierbei sind angemessene Recherche-Möglichkeiten vorzusehen.

3.2.4.4 Machbarkeit eines Forschungsvorhabens prüfen

Zweck und Anwendungsbereich: Für die Planung eines neuen Forschungsvorhabens ist eine realistische Abschätzung erreichbarer Fallzahlen in der geplanten Laufzeit extrem wichtig. Innerhalb eines wissenschaftlich vertretbaren Rahmens können dabei die Ein- und Ausschlusskriterien so lange angepasst werden, bis die retrospektive Analyse von Bestandsdaten eine ausreichende Fallzahl signalisiert.

Prozessablauf: Zunächst wird in bestehenden Datensätzen nach Patienten gesucht, die zu den für eine Studie definierten Ein- und Ausschlusskriterien passen. Das Ziel der Machbarkeitsprüfung ist eine Abschätzung, ob in einem bestimmten Zeitraum in der Zukunft ausreichend Patienten zu erwarten sind, auf die die definierten Ein- und Ausschlusskriterien zutreffen. Die Abfrage kann sich auf historische Daten beziehen, die in vielen Fällen die bestmögliche Schätzung für eine Machbarkeit in der Zukunft erlauben. Solche Abfragen können daher auch mit anonymisierten Datensätzen durchgeführt werden, zudem sollte nur die Anzahl der passenden Patienten zurückgemeldet werden. Eine Machbarkeitsprüfung kann im Rahmen der Entwicklung eines realistischen Studiendesigns auch mehrfach mit leicht veränderten Abfragekriterien durchgeführt werden.

3.2.4.5 Rekrutierung unterstützen

Zweck und Anwendungsbereich: Für neue Studien oder Register werden Patienten oder Probanden mit geeigneten Merkmalen benötigt. Wenn in bestehenden Datenbanken die Daten geeigneter und ansprechbarer Probanden gespeichert sind, so sollten diese im Rahmen einer Rekrutierungsunterstützung gefunden und mit den passenden Kontaktdaten verknüpft werden. Relevante Datensammlungen können sich in einem klinischen Modul oder Forschungsmodul befinden. Auch die Analysedaten eines Biobankenmoduls können hierfür geeignet sein.

Prozessablauf: Bestehende Datenbanken werden auf Grund von definierten Ein- und Ausschlusskriterien nach aktuell kontaktierbaren Probanden mit passenden Daten durchsucht. Das Ergebnis ist eine Vorschlagsliste, auf deren Basis die Probanden vom behandelnden Arzt oder, sofern eine diesbezügliche Einwilligung vorliegt, auch aus dem Forschungsprojekt direkt angesprochen werden.

3.2.4.6 Daten auswerten

Zweck und Anwendungsbereich: Vorhandene Daten werden statistisch ausgewertet. Dies kann auf unterschiedlichen methodischen Niveaus geschehen, z.B. als beschreibende Statistik zur medizinischen Qualitätssicherung (oder Benchmarking) und zur Hypothesengenerierung (oder Data Mining) oder als Inferenzstatistik zur Prüfung vorher formulierter Hypothesen.

Prozessablauf: Der Datenmanager, der für die Datenbank verantwortlich ist, kann einfache Auswertungen direkt durch Datenbankabfragen erstellen. Ansonsten wird in der Regel ein Datenexport von der Datenbank in ein für die verwendete Statistiksoftware nutzbares Dateiformat durchgeführt; dabei wird auf Datensparsamkeit und Anonymität geachtet.

3.2.4.7 Daten an Forscher weitergeben

Zweck und Anwendungsbereich: Daten werden für externe Forschungsprojekte oder einen externen Datenabgleich gemäß den Regeln des Forschungsverbunds bereitgestellt; dabei wird auf Datensparsamkeit und – soweit Personenbezug nicht erforderlich ist – auf Anonymität geachtet.

Prozessablauf: Daten werden in eine für die Weitergabe geeignete Datei exportiert. Ggf. kann auch ein beschränkter Online-Zugriff auf eine Datenbank gewährt werden.

3.2.5 Besonderheiten

Bei klinischen Studien nach AMG oder MPG, bei Bilddatenbanken und bei Biobanken gibt es zusätzlich zu den oben beschriebenen einige spezielle Prozesse, die bei anderen Typen medizinischer Forschung nicht auftreten. Besondere Prozesse erfordert zudem der Einsatz verteilter IT-Infrastrukturen, die in den letzten Jahren unter den Stichworten „Grid-“ und „Cloud-Computing“ eingeführt wurden.

3.2.5.1 Besonderheiten bei klinischen Studien

Hier gibt es einige durch die GCP-Verordnung vorgeschriebene Besonderheiten; diese betreffen z.B.

- die Aufnahme in eine Studie,
- das Erheben von Studiendaten,
- das Auswerten der Studiendaten,
- das Management unerwarteter Ereignisse,
- die Qualitätssicherung der Daten,
- das Archivieren der Daten,
- die Einbindung des Sponsors sowie
- die Überwachung durch die zuständige Behörde

Diese Anwendungsfälle werden in Kapitel 5.2.2 ausführlicher beschrieben.

3.2.5.2 Besonderheiten bei Biobanken

Die Besonderheiten bei Biobanken im Vergleich zu anderen Forschungsprojekten oder Komponenten eines Forschungsverbunds beruhen

- auf dem Umgang mit biologischem Material (Proben und daraus erzeugten Derivaten) sowie
- auf dem unvermeidlichen Entstehen umfangreicher genetischer Informationen über den Spender der Probe.

Der physische Umgang mit Proben reicht von der Materialgewinnung über Probeneinlagerung und Aliquotierung bis zur Vernichtung von Restmaterial, wenn dieses nicht mehr benötigt wird oder der Spender seine Einwilligung widerruft. Die Probennutzung besteht in Analysen, die in der Biobank selbst, oft aber auch in externen Speziallabors durchgeführt werden. Eine Probenweitergabe an andere Forschungsprojekte ist oft in der Zweckbestimmung der Biobank vorgesehen.

Dieser Problembereich wird in Kapitel 5.4 aufgegriffen, genauere Beschreibungen aller Anwendungsfälle und Prozesse sind in [2] zu finden.

3.2.5.3 Besonderheiten bei Bilddatenbanken

Bilddaten gehören bei vielen medizinischen Fragestellungen sowohl für Behandlungszwecke als auch für die wissenschaftliche Verwendung zum Datensatz einer Person. Zu den bildgebenden Verfahren gehören Röntgen, auch als Computer-Tomografie (CT), Kernspin-Tomografie (Magnetresonanz-Tomografie, MRT), Szintigrafie, Positronen-Emissionstomografie (PET) oder andere nuklearmedizinische Verfahren, sowie Sonografie (Ultraschall), Endoskopie und andere optische oder fotografische Verfahren. Aus medizinischen Schichtbildern, insbesondere von CT und MRT, können auch dreidimensionale Bilder rekonstruiert werden, die einen sehr genauen und plastischen Einblick in das Körperinnere gestatten und manchmal die betroffene Person erkennen lassen können. Bilddaten enthalten in der Regel einen Metadatensatz nach dem DICOM-Standard, in dem unter anderem auch identifizierende oder andere für

das Individuum charakteristische Daten enthalten sind. Oft sind, z.B. bei Ultraschallbildern, solche Daten auch direkt in das Bild „eingebrannt“,.

Bilder dienen primär zur Befundung und werden somit zunächst im direkten Behandlungszusammenhang verwendet. Hierzu gehört in einem Forschungsverbund oder einer klinischen Studie auch die externe Befundung durch einen Experten, z.B. einen Referenzradiologen oder auch im Rahmen eines Expertenforums. Bilder werden aber auch als Referenzmaterial für die Befundung anderer Patienten herangezogen, auch in einem Expertenforum (s. Kap. 3.2.4.2 und 3.2.4.3). Darüber hinaus sind Bilder als Anschauungsmaterial für Lehrzwecke unverzichtbar.

Aus technischen Gründen – wegen besonderer Datenformate, aber auch wegen des großen Umfangs von Bilddateien – werden Bilder oft nicht zusammen mit anderen Daten, sondern in separaten Bilddatenbanken gespeichert. Hier müssen natürlich Verweisinformationen vorgesehen sein, die eine korrekte Zuordnung der Bilder zu den sonstigen Daten ermöglichen. Ansonsten werden Bilddaten aus Sicht der Prozessabläufe wie andere medizinische Daten verwaltet und genutzt, wobei auf die vorgesehenen Anonymisierungs- oder Pseudonymisierungsverfahren besonders geachtet werden muss (s. Kap. 6.5.2.3).

3.2.5.4 Besonderheiten beim Einsatz von Grid- oder Cloud-Computing

Aufgrund stetig steigender Datenmengen, gerade in den Bereichen der Bildgebung, der genetischen Forschung und der Verarbeitung von Freitexten (Textmining), und den damit einher gehenden ressourcenintensiven Verarbeitungs- und Auswertungsvorgängen, wurden in den letzten Jahren vermehrt verteilte Infrastrukturen in der biomedizinischen Forschung aufgebaut und für die Datenverarbeitung genutzt[6]. Für die Verarbeitung sensibler medizinischer Daten im Grid oder in der Cloud ergeben sich dabei besondere Herausforderungen: Zum einen steigt mit der zunehmenden Menge der zu einem Patienten gespeicherten Daten auch das Reidentifizierungspotenzial, zum anderen sind Daten in verteilten Infrastrukturen schwerer vor unberechtigten Zugriffen zu schützen.

Um sensible Gesundheitsdaten auch in verteilten Infrastrukturen datenschutzkonform verarbeiten zu können, sind daher sowohl Maßnahmen und Prozesse zur weiteren Absenkung des Schutzbedarfs der Daten notwendig als auch organisatorische und ggf. vertragliche Absicherungen eines ausreichenden Schutzniveaus im Grid bzw. in der Cloud. Weitere Hinweise zu diesen Maßnahmen und Voraussetzungen finden sich in der Beschreibung des ID-Managements in Kapitel 6.1.3.7. Konkrete Umsetzungsbeispiele sind bzw. werden

6 z.B. www.medigrid.de, www.pneumogrid.de, www.eu-acgt.org, www.cloud4health.de, www.labimi-f.med.uni-goettingen.de

in den Ergebnisdokumenten der Projekte PneumoGrid und cloud4health beschrieben[7].

3.3 Formale Beschreibung der Anwendungsfälle

Für die informationstechnische Umsetzung von Anwendungsfällen ist eine formalisierte Beschreibung hilfreich; diese unterstützt ein systematisches Vorgehen und die Strukturierung des Gesamtsystems, hilft beim Aufdecken von Inkonsistenzen und schließlich auch bei der Überprüfung der Vollständigkeit der Implementierung. Ein gut geeignetes methodisches Hilfsmittel ist die Modellierungssprache UML[8], die insbesondere die Diagrammtypen Use-Case-Diagramm und Sequenzdiagramm verwendet.

Das methodische Vorgehen bei der Modellierung der Anwendungsfälle sowie illustrative Beispieldiagramme und ein umfangreiches UML-Modell sind im Anhang zu finden, der online zur Verfügung gestellt wird.[9]

7 s. www.pneumogrid.de und www.cloud4health.de
8 Unified Modeling Language (http://www.uml.org)
9 siehe www.tmf-ev.de/datenschutz-leitfaden

4 Rechtliche und ethische Rahmenbedingungen

4.1 Interesse der Patienten – Nutzen für die Forschung[10]

Medizinischer Fortschritt ist nicht ohne die Erhebung, Verarbeitung und Auswertung medizinischer Daten und Proben zu erreichen. Bei der Zusammenführung solcher Daten und Proben zur langfristigen Nutzung sind zunächst scheinbar widerstreitende Interessen zu berücksichtigen. An erster Stelle steht der wichtigste und ausnahmslos anzunehmende Wunsch jedes Patienten, seine individuelle Gesundheit wiederherzustellen bzw. zu erhalten und hierfür eine optimale Behandlung zu bekommen. An zweiter Stelle – in Einzelfällen bereits dem ersten entgegenstehend – steht der ebenso anzunehmende Wunsch jedes Patienten, so wenig wie möglich durch den Heilungs- und Behandlungsprozess beeinträchtigt zu werden. Das oberste Ziel der Forschung, bessere Behandlungsmöglichkeiten zu finden, ist somit zu den Wünschen der Patienten zumeist komplementär. Auf dem Weg dahin benötigen Forscher Behandlungsdaten und biologische Proben von Patienten, um daraus epidemiologische Informationen zu generieren, neue Behandlungsmethoden zu bewerten oder Analyseergebnisse von biologischen Proben mit den Verlaufsdaten der Erkrankungen zu korrelieren. Im Ergebnis kann häufig die Behand-

10 Dieses Kapitel stellt eine Überarbeitung des Kapitels „1 Problemstellung“ des einführenden Abschnitts der ersten Version des generischen Datenschutzkonzepts dar [1, S. 2f.]. Einzelne übernommene Formulierungen wurden der Lesbarkeit halber nicht separat gekennzeichnet.

lung künftiger Patienten verbessert und im besten Fall sogar ein unmittelbarer Vorteil an individuelle Studienteilnehmer zurückgegeben werden.

Alle diese Wünsche, Ziele und Möglichkeiten führen dazu, dass der Datenschutz in der medizinischen Forschung eine herausragende Bedeutung hat und haben muss. Es ist im gemeinsamen Interesse von Patienten, behandelnden Ärzten und Wissenschaftlern, alle Gefährdungen oder Beeinträchtigungen der Patienten, die mit der Einwilligung, Diagnostik und Behandlung im Rahmen eines Forschungsverbunds für die Medizin verknüpft sind, so gering wie möglich zu halten. Zu diesem „Gefährdungspotenzial" gehört natürlich auch der ungeeignete Umgang mit personenbezogenen Daten: Selbst ein unfreiwilliger, potenzieller oder latenter Bruch der ärztlichen Schweigepflicht bzw. die Missachtung von Datenschutzbestimmungen in diesem Zusammenhang kann das Verhältnis zwischen Patient und Arzt stören und den Bruch des Vertrauensverhältnisses zwischen Patient und Forschungsverbund zur Folge haben. Als Resultat wären Patienten nicht mehr bereit, dem Forschungsverbund ihr Vertrauen in Form ihrer Mitarbeit zu gewähren, und den Forschungsprojekten wäre ihre Existenzgrundlage und Daseinsberechtigung entzogen.

Die Forschungsverbünde sind daher aus eigenem Interesse an einer alle Mitglieder umfassenden, praktikablen, transparenten und kontrollierbaren Lösung interessiert, die hilft, die Datenschutzbelange ihrer Patienten nachhaltig zu wahren.

4.2 Datenschutzrechtliche Grundlagen

4.2.1 Informationelle Selbstbestimmung

Medizinische Forschung muss immer einen Ausgleich zwischen dem Interesse der Allgemeinheit an medizinischem Fortschritt und den Individualinteressen der beteiligten Probanden hinsichtlich der informationellen Selbstbestimmung anstreben. Die für die Forschung notwendigen Daten werden regelmäßig als besondere personenbezogene Daten gemäß § 3 Abs. 9 BDSG (Gesundheitsdaten) anzusehen sein. Die für diese Datenkategorie speziell formulierten Forschungsklauseln in § 13 Abs. 2 und § 28 Abs. 6 BDSG normieren für den Regelfall einen Vorrang der Verwendung anonymisierter und pseudonymisierter Daten und der Einholung einer Einwilligung. Nur wenn der Forschungszweck auf diesen Wegen nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann, kann eine gesetzliche Verwendungserlaubnis nach § 13 Abs. 2 Nr. 6 und § 28 Abs. 6 Nr. 4 BDSG greifen [11].

Wenn klinische Daten für ein Forschungsprojekt erhoben werden, ist im Regelfall die Aufklärung der Patienten und das Einholen einer Einwilligung möglich. Anders sieht es hingegen aus, wenn die Daten bereits zu einem früheren Zeitpunkt im Rahmen der Behandlung der Patienten erhoben wurden und

jetzt für die Forschung nutzbar gemacht werden sollen. Einige Landeskrankenhausgesetze (LKG) erlauben die Nutzung und Verarbeitung solcher Daten innerhalb der behandelnden Einrichtung auch zum Zwecke der Forschung (z.B. Art. 27 [4] BayKrG). Allerdings ist zu beachten, dass sich auch zusätzliche Anforderungen durch landesspezifische Gesetze ergeben können, so z.B. eine lokale Pseudonymisierung in Verbundforschungsprojekten (vgl. § 25 [3] LKG Berlin). Sollen die Daten aber zum Zwecke der Forschung weitergegeben werden, bieten selbst weitgehende Regelungen in den Landeskrankenhausgesetzen üblicherweise keine gesetzliche Grundlage. Hier können die speziellen Forschungsklauseln der Datenschutzgesetze greifen, wenn die Übermittlung der Daten zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an dem Forschungsvorhaben das Interesse des Betroffenen an dem Ausschluss einer nicht vereinbarten Nutzung seiner Daten erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit einem unverhältnismäßigen Aufwand zu erreichen ist. Hierzu ist allerdings konkret zu begründen, warum das Forschungsvorhaben nicht mit anonymen oder pseudonymen Daten umgesetzt werden kann und die Einholung der Einwilligung der betroffenen Patienten unzumutbar ist. Zusätzlich kann ein Genehmigungsvorbehalt vorgesehen sein (z.B. § 33 HDSG). Die Höhe der hierfür gesetzlich vorgeschriebenen Hürden reflektiert zudem die Auflagen der ärztlichen Schweigepflicht nach § 203 Abs. 1 StGB.

Die von der TMF beauftragten Rechtsgutachter Roßnagel, Hornung und Jandt formulieren dies zusammenfassend so: „Die forschungsspezifischen Datenschutzregelungen lösen somit den regelmäßig bestehenden Konflikt zwischen den konkurrierenden Grundrechten der Forschungsfreiheit gemäß Art. 5 Abs. 3 GG der Daten verarbeitenden Forschungsstellen und dem Recht auf informationelle Selbstbestimmung der Probanden gemäß Art. 2 Abs. 1 und Art. 1 Abs. 1 GG, indem sie über die Einwilligungsmöglichkeit und die strenge Zweckbindung zu einem interessensgerechten Ausgleich der Grundrechte führen.“ [11, S. C11]

Einen Sonderfall stellt die Mitnutzung von Daten für die Forschung dar, die zu einem anderen Zweck, z.B. dem der Behandlung oder Abrechnung einer Behandlung, erhoben wurden. Das Bundessozialgericht (BSG) kommt in seinem Urteil vom 10.12.2008 zur Weitergabe von Patientendaten durch Leistungserbringer an private Abrechnungsstellen zu dem Schluss, dass die datenschutzrechtlichen Regelungen im SGB so umfassend und detailliert ausgeführt sind, dass eine nachgeordnete Anwendung des Datenschutzrechts nicht mehr im Sinne des Gesetzgebers sein könne [12]. Dementsprechend wären die im SGB aufgeführten Daten und insbesondere die Sozialdaten bei den Leistungserbringern gemäß § 284ff SGB V auch bei Vorliegen einer schriftlichen Einwilligung nicht anders zu verwenden, als dies im SGB konkret vorgesehen ist. Bei dieser Auslegung stützt sich das BSG wesentlich auf den Umstand, dass der Gesetzgeber an anderer Stelle die Zulässigkeit einer auf eine Einwilligung gestützten Datenübermittlung durch Leistungserbringer ausdrücklich geregelt

hat, so z.B. für den Datenaustausch zwischen Hausarzt und anderen Leistungserbringern (§ 73 Abs. 1b Satz 1 und 2 SGB V) [12, Abs. 35]. Dass der Gesetzgeber in § 291a (8) SGB V für ganz bestimmte Datenverwendungen eine Einwilligung explizit ausgeschlossen hat (vgl. Kap. 4.3.2), wird in dem Urteil hingegen nicht gewürdigt. Dieser explizite Ausschluss einer Einwilligung als Rechtsgrundlage würde eher die Schlussfolgerung nahe legen, dass der Gesetzgeber grundsätzlich von der Möglichkeit einer Einwilligungsregelung ausgeht.

In ihrem Rechtsgutachten zur Mitnutzung von Versorgungsdaten in der Forschung kommen Roßnagel und Mitarbeiter zu dem Schluss, dass die Abgeschlossenheit der Regelungen zum Datenschutz im SGB vom BSG nur für die §§ 284ff SGB V schlüssig dargelegt ist. Somit wäre auch nur für diesen Ausschnitt des SGB der Ausschluss einer Einwilligung als Rechtsgrundlage für die Nutzung in der Forschung anzunehmen [11, S. C7]. Zudem weisen die Gutachter darauf hin, dass aus datenschutzrechtlicher Perspektive zwei Kategorien von Daten zu unterscheiden sind: Zum einen gibt es Daten, die für Zwecke der Versorgung erhoben und dokumentiert werden und für die die Regelungen des ärztlichen Berufsrechts und ergänzend des Datenschutzrechts gelten. Davon zu unterscheiden sind die Leistungsdaten als krankenversicherungsrechtliche Sozialdaten, die der Abrechnung von Leistungen der Leistungserbringer im weitesten Sinne dienen. Nur für den Umgang mit letzteren, so die Gutachter, könnten die abschließenden Regelungen des Zehnten Kapitels des SGB V herangezogen werden. Für die Versorgungsdaten seien die Regelungen der § 284ff. SGB V nicht anwendbar, auch wenn ein Datum, wie z.B. die in § 301 Abs. 1 Satz 1 Nr. 3 SGB V genannte Diagnose, inhaltlich in diesen Regelungen erwähnt ist. Eine abschließende Regelung für den Umgang mit Diagnoseinformationen im SGB würde deren Verwendung zu medizinischen Zwecken zu sehr einschränken und sei daher nicht vom Gesetzgeber intendiert [11, S. C8]. Somit bleibt aus Sicht der Gutachter eine Verwendung von Versorgungsdaten auf Basis einer Einwilligung grundsätzlich möglich, vorausgesetzt dass die Daten primär zum Zwecke der Versorgung erhoben wurden und allenfalls sekundär auch für die Abrechnung von Leistungen verwendet werden.

4.2.2 Grenzen von Einwilligungsszenarien

Die rechtlich zulässige Verwendung medizinischer Daten, die die informationelle Selbstbestimmung der Patienten wahren muss, setzt, von wenigen Ausnahmen abgesehen, das Vorliegen einer Einwilligungserklärung voraus. Diese muss freiwillig und ohne Sorge um mögliche Nachteile im Falle einer Verweigerung gegeben werden. Bei der Gestaltung des Aufklärungs- und Einwilligungsprozesses ist zu berücksichtigen, dass sich Patienten aufgrund ihrer Erkrankung von dem behandelnden Personal abhängig fühlen können, das sie um eine Einwilligung bittet. Entsprechend sollte das Gespräch bewusst ergebnisoffen geführt werden. Jede Vermittlung einer Erwartungshaltung in Bezug auf die Antwort des Patienten ist sorgfältig zu vermeiden.

Die Erklärung der Einwilligung muss bestimmt sein, so dass klar zu erkennen ist, unter welchen Bedingungen sich die betroffene Person mit der Erhebung, Verarbeitung oder Nutzung welcher Daten einverstanden erklärt. Aus diesem Grund sind weder Blankoeinwilligungen noch pauschal gehaltene Erklärungen, die den Betroffenen die Möglichkeit nehmen, die Tragweite ihres Einverständnisses zu überblicken, ausreichend. Die Anforderungen an die Bestimmtheit sind umso höher, je größer die Tragweite für die Rechte und Freiheiten der betroffenen Person sind. Gemäß § 4a Abs. 3 BDSG bestehen erhöhte Anforderungen an die Bestimmtheit, wenn sich die Verwendung auf besondere Daten im Sinne des § 3 Abs. 9 BDSG bezieht. Dies schließt explizit Gesundheitsdaten ein. Somit muss für die Einwilligenden klar erkennbar sein, welche Daten, in welcher Form, von wem, wie lange und wofür verarbeitet oder genutzt werden.

Je konkreter die Einwilligung formuliert ist, desto einschränkender und unter Umständen auch problematischer ist sie für die Forschung, und dies gleich in mehrfacher Hinsicht: Je konkreter der Zweck angegeben wird, desto präziser kann auch der notwendige Datensatz, der für die Verarbeitung erforderliche Personenkreis und die hierfür benötigte Projektlaufzeit bestimmt werden. Im Umkehrschluss geht eine zweckoffenere Erhebung und Speicherung im Regelfall auch mit einer geringeren Einschränkbarkeit des Datenumfangs, einer längeren Vorhaltung der Daten und einem größeren mit ihrer Verarbeitung betrauten Personenkreis einher. Dabei ist es sogar häufig auch im Interesse schwer erkrankter Patienten, dass ihre Daten nicht nur einem Forscher mit seinen Spezialinteressen zur Verfügung stehen, sondern von möglichst vielen Experten zur Verbesserung der Behandlungschancen genutzt werden.

Dass es in der medizinischen Forschung oft schwer ist, sich auf eine konkret benennbare Fragestellung zu beschränken, ist weithin anerkannt [13]. Häufig wird daher auch akzeptiert, wenn lediglich krankheitsbezogene Einschränkungen gemacht werden. Ausnahmen hierzu stellen klinische Prüfungen zu Arzneimitteln oder Medizinprodukten dar, die aufgrund der regulatorischen Vorgaben und des geforderten Qualitätsniveaus auf eine Festlegung der Auswertung vor der Datenerhebung angewiesen sind. Aber auch hier kann eine längerfristige Speicherung der wertvollen Daten für zusätzliche Fragestellungen, z.B. zur Generierung neuer Hypothesen, sinnvoll sein. Die Konkretheit der Zweckbezogenheit dient letztlich nur so lange ihrem Ziel der informationellen Selbstbestimmung, wie die Einschränkungen der Forschungsfragestellung von der Mehrheit der Patienten auch nachvollzogen und verstanden werden können. Somit kann auch das Gebot der Verständlichkeit der Einwilligungserklärung schon eine Aufweichung des Prinzips der möglichst engen Definition der Zweckbezogenheit bedeuten. Eine Einschränkung der Forschung auf eine konkrete Unterform der Leukämie wird einem Patienten kaum einen Informationsgewinn bescheren, wenn er diese Unterform nicht ausreichend genau von dem Oberkonzept „Leukämie“ unterscheiden kann.

Jedem Patienten ist hingegen die Unterscheidung zwischen einer zeitlich unbeschränkten Speicherung und einer auf fünf Jahre beschränkten unmittelbar möglich. Ebenso können Patienten zwischen einer Nutzung der Daten nur an einem Klinikum oder auf nationaler oder gar europäischer Ebene unterscheiden. Die mit einer zeitlich unbeschränkten Speicherung einhergehenden Risiken sind jedoch u.U. schwer einschätzbar.

Während eine in Grenzen zweckoffene Erhebung, Speicherung und Verarbeitung medizinischer Daten dem Prinzip einer informierten Einwilligung häufig nicht direkt entgegensteht, verdienen die damit regelmäßig verbundenen Verschiebungen der organisatorischen Rahmenbedingungen eine gesonderte Betrachtung. Die klare Unterscheidbarkeit unterschiedlicher organisatorischer Vorgaben in den Augen der Patienten, wie z.B. der Zeitdauer der Speicherung, empfiehlt diese für die Berücksichtigung in einer abgestuften Einwilligungserklärung [5, S. 97][11]. Auch die Methodik der abgestuften Einwilligungserklärung führt jedoch nicht automatisch zu einer ausreichenden Wahrnehmung bzw. einem informierten Verständnis aller Risiken durch die Patienten.

Mit der verstärkt wahrgenommenen Bedeutung der Biobank-gestützten Forschung in den letzten Jahren ist die Diskussion um eine mögliche Lockerung der Zweckbezogenheit der Einwilligung unter dem Stichwort „broad consent“ erneut und kontrovers geführt worden. Der Deutsche Ethikrat hat in einer Empfehlung zu Humanbiobanken für die Forschung gar gesetzlich geregelte Rahmenbedingungen, wie z.B. ein Biobankgeheimnis, gefordert, welches zusammen mit anderen Regelungen eine zweckoffene Einwilligung ermöglichen sollte [15]. Da bisher jedoch völlig offen ist, ob und in welcher Form der Gesetzgeber diesen Vorschlag aufnimmt, bleibt in jedem Einzelfall zu prüfen und abzuwägen, ob der Grad der Bestimmtheit einer Einwilligung den Forschungsinteressen und der Informiertheit der Probanden noch gerecht wird. Risiken, die durch eine längerfristige, vergleichsweise zweckoffene und breit nutzbare Speicherung medizinischer Daten entstehen, sind, wie in dem vorliegenden Leitfaden dargestellt, durch entsprechende technische und organisatorische Maßnahmen und eine langfristig klar geregelte Verantwortlichkeit auszubalancieren (vgl. Kap. 6.7). Der Arbeitskreis Medizinischer Ethik-Kommissionen in Deutschland (AK EK) hat für Biobanken entsprechende Mustertexte zur Aufklärung und Einwilligung veröffentlicht.[12]

Grundsätzlich ist zu beachten, dass eine allgemein formulierte Zweckbestimmung und die entsprechende Einwilligung in eine offenere spätere Nutzung von Proben und Daten immer nur dann eine ausreichende Rechtsgrundlage

11 Der Nationale Ethikrat hat in der Stellungnahme „Biobanken für die Forschung“ die abgestufte Einwilligung sogar für verzichtbar erklärt, das Fehlen von Wahlmöglichkeiten verletze nicht das Selbstbestimmungsrecht [14, S. 15].

12 siehe http://www.ak-med-ethik-komm.de/formulare.html

für die Forschung bieten können, wenn die Einholung späterer zusätzlicher Einwilligungen aus technischen oder organisatorischen Gründen nicht machbar ist. In bestimmten Fällen kann für die Rekontaktierung beispielsweise ein Abgleich der Daten mit Melderegistern notwendig sein. Hier ist zu prüfen, ob dies im konkreten Fall rechtlich möglich ist (vgl. Kap. 4.3.4). Wenn später eine zusätzliche Einwilligung eingeholt werden soll, muss auch für diese Rekontaktierung eine Einwilligung der Probanden vorliegen. Bei der Prüfung der Durchführbarkeit einer solchen weiterführenden Einwilligung ist zudem zu klären, ob diese zu einer zu großen Selektions-Verzerrung (selection bias) führen könnte.

4.2.3 Verantwortlichkeiten

Die Speicherung und Verarbeitung sensibler medizinischer Daten und Proben setzt eine juristisch belastbare und für jeden Patienten nachvollziehbare Regelung der Verantwortlichkeit voraus (s. Kap. 6.6). Bei der Planung einer langfristigen und einrichtungsübergreifenden Datensammlung ist von vornherein auch zu überlegen, welche verlässliche und vertrauenswürdige Institution mit ebenfalls langfristiger Perspektive die Verantwortung im juristischen Sinne übernehmen kann. Dies kann ein von einem Forschungsnetz gegründeter Verein sein, es sind aber auch andere Lösungen und Formen denkbar, die als juristische Person ansprechbar sind. Bei der Initiierung einer Datensammlung aus einem geförderten Forschungsprojekt heraus ist auch an Regelungen nach Auslaufen der Förderung zu denken. In jedem Fall sollte eine mögliche Rechtsnachfolge für die zunächst verantwortliche Institution geprüft werden. Die notwendige Transparenz gegenüber den Probanden erfordert die verständliche Darlegung der Verantwortlichkeiten in der Einwilligungserklärung.

Der verantwortlichen Institution, z.B. dem Forschungsnetz e.V., wird empfohlen, ein Gremium zu schaffen, welches für datenschutzrechtliche Fragen und Entscheidungen zuständig ist (s. Kap. 6.6). Bei der Besetzung dieses „Ausschusses Datenschutz“ ist darauf zu achten, dass Interessenskonflikte soweit möglich vermieden werden. Das Gremium sollte neben der Beratung einzelner Entscheidungen, z.B. welcher Anfrage nach Daten stattgegeben wird, auch für die Ausarbeitung und Fortschreibung der datenschutzrechtlich relevanten Regelwerke und Policies verantwortlich sein. Das Aufgabengebiet des Ausschuss Datenschutz kann z.T. überlappend mit jenem eines betrieblichen oder behördlichen Datenschutzbeauftragten der beteiligten Einrichtungen oder auch eines Forschungsverbunds als juristischer Person sein. Wenn der Forschungsverbund über einen eigenen Datenschutzbeauftragten verfügt, sollte dieser entsprechend auch Mitglied des Ausschuss Datenschutz werden. In Bezug auf die langfristige pseudonymisierte Aufbewahrung von Gesundheitsdaten kommt dem Ausschuss Datenschutz jedoch eine besondere Verantwortlichkeit zu, die im Regelfall eine Besetzung mit mehreren Personen mit ausreichender Sachkenntnis empfehlenswert erscheinen lässt. Somit sollten auch

alle relevanten Entscheidungen mindestens nach dem Vier-Augen-Prinzip getroffen werden.

4.2.4 Anonymisierung und Pseudonymisierung

Das Bundesdatenschutzgesetz definiert in § 3 Abs. 6 BDSG den Vorgang des Anonymisierens und in § 3 Abs. 6a des Pseudonymisierens. Beide Verfahren werden eingesetzt, um die Zuordnung von Daten zu einer bestimmten oder bestimmbaren Person auszuschließen oder zumindest wesentlich zu erschweren. Somit sind beide Verfahren grundsätzlich geeignet, den Schutzbedarf medizinischer Daten abzusenken, bzw. Risiken, die sich aus der Speicherung und Verarbeitung der Daten ergeben, zu minimieren.

Daten sind nach § 3 Abs. 6 BDSG anonymisiert, wenn sie entweder „nicht mehr" oder „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können". Während die erste Option als absolute Anonymisierung bezeichnet wird, ist die letztere realistischerweise die häufigere und wird mit dem Begriff der faktischen Anonymisierung belegt [16]. Grundsätzlich wird von einer Anonymisierung ausgegangen, wenn identifizierende und medizinische Daten getrennt werden, keine Zuordnungsregel mehr existiert und anhand der medizinischen Daten allein keine Reidentifizierung möglich ist. Anonymisierte Daten gelten damit für nicht mehr personenbeziehbar, so dass für sie auch das Datenschutzrecht samt Einwilligungsvorbehalt nicht mehr anzuwenden ist [11, S. C35]. Problematisch im Umgang mit anonymisierten Daten ist, dass sich der Status der Anonymität im Laufe der Zeit ändern kann, z.B. wenn ein Nutzer der Daten aufgrund einer bestimmten Kombination medizinischer und sozialer Daten auf die Identität des zugehörigen Patienten schließen kann. In diesem Falle würde es sich wieder um personenbezogene Daten handeln, die entsprechend der Vorschriften der Datenschutzgesetze des Bundes und der Länder zu behandeln wären. Problematisch an einem solchen Szenario ist, dass sich im Vorfeld nicht immer ausreichend präzise einschätzen lässt, ob und wann ein solcher Fall eintreten kann. Zur Vorbeugung wird daher empfohlen, auch anonymisierte Datenexporte nur zweckbezogen an definierte Nutzerkreise abzugeben und insbesondere auf die freie Verfügbarmachung medizinischer Daten im Internet in so genannten Public-Use-Files zu verzichten.

Nach § 3 Abs. 6a BDSG ist Pseudonymisieren das „Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." Im Unterschied zu anonymisierten Daten besteht bei pseudonymisierten Daten noch eine Zuordnungsregel zu den Identitätsdaten der betroffenen Personen. Die Zuordnungsregel ist jedoch nicht allen Nutzern der Daten bekannt, da sonst der Zweck der Pseudonymisierung nicht erreicht würde. Somit muss

hinsichtlich der Datenschutzanforderungen unterschieden werden zwischen Nutzerkreisen, die die Zuordnungsregel kennen und solchen, die sie nicht kennen. Für die erste Gruppe handelt es sich offensichtlich um personenbezogene Daten gemäß dem Datenschutzrecht. In Bezug auf die Einordnung der Daten für die zweite Nutzergruppe gibt es jedoch unterschiedliche Auffassungen. Roßnagel kommt in einem für die TMF erstellten Rechtsgutachten zu dem Schluss, dass pseudonymisierte Daten für Nutzer ohne Zugriff auf die Zuordnungsregel anonymisierten Daten gleichgestellt werden können, wenn „nach der allgemeinen Lebenserfahrung oder dem Stand der Wissenschaft die Zuordnung der Daten zu einer Person praktisch ausscheidet" [11, S. C33]. Eine andere Position wird von Bizer vertreten, der die Möglichkeit einer „relativen Anonymisierung" für Nutzer ohne Zugriff auf die Zuordnungsregel grundsätzlich verneint [17, RN 217; 18]. Auch Roßnagel weist aber darauf hin, dass pseudonymisierte Daten z.B. prinzipiell nicht in Public-Use-Files veröffentlicht werden sollten, da es dann immer Nutzer gibt, die die Zuordnungsregel kennen und damit das Prinzip der Informationsaufteilung umgehen können [11, S. 36]. Zudem bedeutet das Vorhandensein einer Zuordnungsregel auch, dass ein Datensatz hinsichtlich seines inhärenten Reidentifizierungspotenzials nicht abschließend beurteilt werden kann, da grundsätzlich weitere Daten, z.B. aus Follow-ups, zugeordnet werden können. Im Ergebnis empfiehlt auch Roßnagel, den Umgang mit pseudonymisierten Daten am Datenschutzrecht auszurichten, da die Gefahr einer Reidentifizierung zumeist nicht ausreichend sicher ausgeschlossen werden kann.

Ein Sonderfall der Pseudonymisierung besteht dann, wenn eine kryptographische Einwegfunktion zur Generierung der Pseudonyme verwendet wird. In diesem Fall ist kein Schlüssel zur Umkehrung der Pseudonymisierung vorhanden, oder dieser kann bei Nutzung eines asymmetrischen Verschlüsselungsverfahrens vernichtet werden. Somit erlaubt auch die Kenntnis der Zuordnungsregel keine direkte Zuordnung des Pseudonyms zu den identifizierenden Daten. Hierfür hat sich auch der Begriff „Einwegverschlüsselung" etabliert. Es stellt sich dabei die Frage, ob Daten mit nur noch unidirektional vorhandener Zuordnungsregel anders zu bewerten sind, als medizinische und identifizierende Daten, bei denen eine Zuordnung zumindest von einer bestimmten Benutzergruppe in beide Richtungen vorgenommen werden kann. Grundsätzlich wird bei solchen asymmetrischen Verfahren empfohlen, diese so ausprobiersicher zu machen, dass bis auf einen definierten Nutzerkreis niemand Probeverschlüsselungen mit beliebigen identifizierenden Daten machen kann. Dies bedeutet, dass mindestens einer der verwendeten Schlüssel geheim gehalten wird und der Zugang zu dieser Funktion nur autorisierten Nutzern gewährt wird. Trotzdem wird mindestens eine Nutzergruppe weiter Zugang zu dem Verfahren haben und entweder Probeverschlüsselungen vornehmen oder sogar identifizierende Daten als Nutzdaten an dem Verschlüsselungsverfahren „vorbei" schicken können, so dass auf der anderen Seite des Verfahrens identifizierende Daten mit dem asymmetrisch generierten Pseu-

donym im Zusammenhang auftauchen. Abgesehen von solchen Risiken werden aber auch solche asymmetrischen Verfahren hauptsächlich dann eingesetzt, wenn den einmal pseudonymisierten Daten später noch weitere Daten zugeordnet werden sollen. Damit fallen solche Daten auch bezüglich der Problematik des nicht abschließend zu beurteilenden inhärenten Reidentifizierungsrisikos in die gleiche Kategorie, wie die zuvor beschriebenen pseudonymisierten Daten. Entsprechend kommt auch Roßnagel in seinem Gutachten [11, S. C39] zu dem Schluss: „Solange die Identitätsdaten zu den verschlüsselten Behandlungsdaten noch vorhanden sind, besteht grundsätzlich ein höheres Risiko der Reidentifizierung, als wenn die Identitätsdaten vernichtet worden wären. Besteht darüber hinaus eine Zuordnungsregel, sind die Daten pseudonymisiert und nicht anonymisiert." Demzufolge sind pseudonymisierte Daten unabhängig von der Verwendung einer Einwegfunktion zur Generierung des Pseudonyms von ihrem rechtlichen Status her zwischen den personenbezogenen und den anonymen Daten einzuordnen.

Einwegfunktionen ermöglichen die Generierung des immer gleichen Pseudonyms bei identischen Ausgangsdaten. Dies ermöglicht die Erstellung von Pseudonymen auf Basis der identifizierenden Daten von Patienten und erlaubt somit gleichzeitig, auf eine zentrale und langfristige Speicherung der identifizierenden Daten zu verzichten. Somit entfällt die Notwendigkeit, die identifizierenden Daten langfristig und z.B. mit Hilfe eines Treuhänders zu schützen. Auf der anderen Seite entfällt in einem solchen Szenario regelmäßig die Möglichkeit, die beteiligten Patienten zu einem späteren Zeitpunkt sicher zu kontaktieren. Ein weiterer und weniger offensichtlicher Nachteil ist die eingeschränkte langfristige Sicherheit des Pseudonyms. Dessen Sicherheit fußt auf der kryptographisch gesicherten Unumkehrbarkeit des verwendeten Algorithmus, die jedoch nach aller Erfahrung nicht dauerhaft gegeben sein wird.

Die vergleichende Betrachtung der beiden Verfahren der Anonymisierung und Pseudonymisierung zeigt, dass sich der Sicherheitsvorteil der Anonymisierung aufgrund der heute häufig benötigten umfangreichen medizinischen Datensätze mit ihrem inhärenten Reidentifizierungsrisiko stark relativiert. Bei der Wahl des passenden Verfahrens zur Absenkung des Schutzbedarfs medizinischer Daten ist aber noch entscheidender, dass viele Anwendungsfälle mit anonymisierten Daten nicht umgesetzt werden können. Neben der Notwendigkeit, klinische Daten mit Hilfe von Follow-ups im langfristigen Verlauf studieren zu können, ist hier auch die Möglichkeit des individuellen Feedbacks z.B. über neue Therapiemöglichkeiten, Risiken oder Zufallsbefunde zu nennen. Ein solches Feedback kann jedoch nur dann die Verwendung pseudonymer statt anonymer Daten rechtfertigen, wenn die Rückmeldung mit den Patienten im Rahmen einer hinreichend bestimmten Einwilligung vereinbart wurde (vgl. auch Kap. 4.4.2). Auch die zunehmend hochselektive Rekrutierung für neue Studien kann nur mit Hilfe pseudonymisiert gespeicherter Daten unterstützt werden. Siehe hierzu auch Kapitel 3.2.3.

4.2.5 Elektronische Datentreuhänderschaft

Die vorliegende Konzeption datenschutzgerechter Lösungen in der medizinischen Forschung sieht für viele Szenarien eine informationelle Gewaltenteilung vor, die durch eine Unabhängigkeit des administrativen Zugriffs auf verschiedene Komponenten und Anteile des Datenbestandes zu realisieren ist. Eine zentrale Komponente dieser verteilten Konzeption ist eine elektronisch geführte Patientenliste, die den Zusammenhang identifizierender Patientendaten (IDAT) zu Pseudonymen (PID) speichert. Die Einbindung eines Treuhänders bedeutet, dass die Verwaltung und Speicherung dieser Informationen bei einer Einrichtung oder Person angesiedelt wird, die rechtlich, räumlich und personell selbstständig und unabhängig ist. Darüber hinaus sollte der Treuhänder auch das Vertrauen der betroffenen Patienten oder Probanden genießen.

Da schon allein die Tatsache, dass ein Patient mit Namen und Anschrift oder anderen identifizierenden Daten in einer solchen Liste gespeichert ist, etwas über eine spezifische Erkrankung des Patienten aussagen kann, sind auch solche Daten als sensibel und schützenswert einzustufen. In besonderen Fällen kann der begründete Wunsch der Probanden bestehen, dass eine solche zentrale Datei beschlagnahmesicher im Sinne des § 97 StPO aufbewahrt wird. Vor diesem Hintergrund wurde in der Vergangenheit für einige Forschungsnetze die Beauftragung eines Notars als Datentreuhänder vorgeschlagen [19, S. 41] und z.T. auch umgesetzt, so z.B. im Kompetenznetz Parkinson[13].

Der von der TMF zur Klärung der Rahmenbedingungen einer elektronischen Datentreuhänderschaft beauftragte Rechtsgutachter Dierks weist zum einen auf das vom Beschlagnahmeschutz und dem komplementären Zeugnisverweigerungsrecht nach § 53 StPO adressierte Verhältnis zwischen Arzt und Patient und zum anderen auf die Thematik des Gewahrsams hin. Beide Aspekte, sowohl das Vertrauensverhältnis als zu schützendes Gut und Ausgangspunkt des Beschlagnahmeschutzes, als auch die Regelungen zum Gewahrsam, können sich für die Forschung als problematisch erweisen [20].

Nach Dierks [20, S. B12] ist zwar davon auszugehen, dass auch ein forschender Arzt zu dem Kreis der potenziell Zeugnisverweigerungsberechtigten des § 53 Abs. 1 Nr. 3 StPO gehört. Das Zeugnisverweigerungsrecht steht ihm jedoch nur zu, soweit es um Informationen geht, die ihm in seiner Eigenschaft als Arzt vom Hilfesuchenden anvertraut worden oder bekannt geworden sind. Maßgeblich ist somit das individuelle Beratungs- und Behandlungsverhältnis zwischen dem Arzt und demjenigen, der seine Hilfe in Anspruch nimmt. Ein forschender Arzt, der kein individuelles Beratungs- oder Behandlungsverhältnis zum Patienten hat, wird sich in einem Strafverfahren im Regelfall nicht auf ein Zeugnisverweigerungsrecht berufen können. In den Fällen, in denen die Forschung im Rahmen eines Behandlungsverhältnisses stattfindet, wie

13 www.kompetenznetz-parkinson.de

dies z.B. im Rahmen klinischer Prüfungen zumeist anzunehmen ist, kann aber auch für den forschenden Arzt ein Zeugnisverweigerungsrecht angenommen werden. Analog kann von einem Zeugnisverweigerungsrecht ausgegangen werden, wenn der forschende Arzt hinzugezogen und in das Behandlungs- und Beratungsverhältnis des Arztes mit seinem Patienten eingebunden wird. Der forschende Arzt wäre dann aber nicht Berufshelfer des behandelnden oder beratenden Arztes nach § 53a StPO, sondern selbst zeugnisverweigerungsberechtigt im Sinne des § 53 Abs. 1 Nr. 3 StPO.

Neben dem individuellen Beratungs- und Behandlungsverhältnis zwischen Arzt und Patient sind aber auch die Regelungen zum Gewahrsam der zu schützenden Daten zu berücksichtigen. Eine relevante Erweiterung der Regelungen zum Gewahrsam wurde im Rahmen des Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG) im Jahre 2003 zur Vorbereitung der Einführung der elektronischen Gesundheitskarte (eGK) eingeführt. Seitdem können Daten auch im Gewahrsam eines Dienstleisters des zeugnisverweigerungsberechtigten Arztes vom Beschlagnahmeschutz umfasst sein. Dierks weist darauf hin, dass der Begriff des Dienstleisters im konkreten Zusammenhang mit der Einführung der eGK und der zugehörigen Telematikinfrastruktur im Gesundheitswesen im Gesetz verankert wurde, dass er aber dem Wortlaut des Gesetzes nach auch unabhängig von der eGK verstanden werden kann und sollte. Demnach wären auch Daten bei einem Dienstleister von einer Beschlagnahme ausgenommen, wenn dessen Beauftragung unabhängig von der Nutzung einer eGK wäre. Vor dem Hintergrund der aktuell eingeschränkten Nutzbarkeit der eGK-Infrastruktur für die Forschung (s. das weiter unten folgende Kap. 4.3.2 zur Gesundheitstelematik) kann dieser Befund für einige Anwendungsfälle der Forschung von Interesse sein. Dierks weist aber auch darauf hin, dass es derzeit zur Interpretation des Dienstleisters nach § 97 Abs. 2 Satz 2 StPO noch keine ausreichend umfangreiche Rechtsprechung gibt, die einen verlässlichen Rechtsrahmen aufspannen würde [20, S. B18].

Somit wäre ein Beschlagnahmeschutz in vertretbarer, jedoch rechtlich nicht abgesicherter Weise über die Aufbewahrung der Patientenliste in elektronischer Form bei einem IT-Dienstleister nach § 97 Abs. 2 Satz 2 StPO zu erreichen, sofern ein eindeutiger Bezug zum spezifischen geschützten Vertrauensverhältnis zwischen Arzt und Patient gegeben ist, aus dem die Daten stammen. Allerdings würde in einem solchen Falle der Dienstleister eine Datenverarbeitung im Auftrag (vgl. § 28 BDSG) übernehmen und wäre gegenüber dem Auftraggeber weisungsgebunden. Metschke und Wellbrock weisen jedoch darauf hin, dass bei einer Datenverarbeitung im Auftrag aufgrund der Weisungsgebundenheit des Auftragnehmers keine ausreichende informationelle Gewaltenteilung erreicht wird. Hierfür muss der Datentreuhänder selbstständige Daten besitzende Stelle sein [19, S. 42]. Die informationelle Gewaltenteilung ist im Regelfall jedoch gerade das Ziel der Einbindung eines Datentreuhänders.

Zu der Frage, ob ein weitergehender Beschlagnahmeschutz durch die Einschaltung eines Notars als Datentreuhänder erreicht werden kann, kommt Dierks allerdings zu einem negativen Ergebnis. Zwar gehören Notare auch zu dem zeugnisverweigerungsberechtigten Personenkreis nach § 53 (1) StPO, allerdings dürfen sie nur über jene Begebenheiten das Zeugnis verweigern, die ihnen in ihrer beruflichen Eigenschaft von ihren Mandanten anvertraut wurden oder bekannt geworden sind und somit das spezifische Vertrauensverhältnis zwischen ihnen und dem auftraggebenden Mandanten betreffen. Informationen über Dritte sind davon nicht automatisch umfasst. Nach Dierks gehört weder die beschlagnahmesichere Aufbewahrung von Dokumenten an sich zu den vom Beschlagnahmeschutz umfassten beruflichen Tätigkeitsbereich eines Notars, noch könnte eine Patientenliste in einem rechtlich sinnvollen Auftrags- und Mandantenverhältnis bei einem Notar so hinterlegt werden, dass dieser sich auf sein Zeugnisverweigerungsrecht berufen könnte. Selbst wenn die Patienten einzeln den Notar mit der Verwaltung ihrer Daten beauftragen würden, müssten sie doch gleichzeitig zur Ermöglichung eines zentralen Zugriffs durch das Forschungsnetz den Notar von seiner Schweigepflicht diesbezüglich entbinden, was wiederum auch die Beschlagnahmesicherheit unterminieren würde. Für Dierks spricht schließlich der Umstand, dass die Mandatierung des Notars gerade der Erreichung eines Beschlagnahmeschutzes dienen soll, für die Beschlagnahmefähigkeit einer Patientenliste beim Notar. Die Übergabe der Patientenliste in die notarielle Verwahrung betrifft dann nicht den Gegenstand seiner typischen und speziellen beruflichen Tätigkeit. Es ist vielmehr von einem Umgehungstatbestand auszugehen, der durch den Schutzzweck des § 97 StPO nicht gedeckt ist [20, S. B22f].

In der Konsequenz ist eine beschlagnahmesichere Einschaltung eines Datentreuhänders in der Forschung nur in wenigen, überwiegend monozentrischen Szenarien erreichbar. Zudem wird in einer solchen Konstellation aufgrund der notwendigen Weisungsgebundenheit des Treuhänders das Prinzip der informationellen Gewaltenteilung durchbrochen. Die Nutzung eines Datentreuhänders ist in vielen Anwendungsfällen und Forschungsfeldern, in denen die Beschlagnahmesicherheit kein hoch priorisiertes Kriterium ist, durchaus sinnvoll und im Sinne einer informationellen Gewaltenteilung positiv zu bewerten. Dies gilt insbesondere dann, wenn es gelingt, eine Institution oder Person für diese Aufgabe zu gewinnen, die bei der relevanten Patientengruppe hohes Vertrauen genießt. Zudem sollte eine solche Stelle datenschutzrechtliche Kompetenz aufweisen und idealerweise auch durch berufsrechtliche Normen an einen vertrauensvollen und sicheren Umgang mit den anvertrauten Daten gebunden sein, wie dies z.B. für Ärzte oder auch Notare gilt.

4.3 Weitere rechtliche Rahmenbedingungen

4.3.1 AMG, MPG

Das Arzneimittelrecht legt in Deutschland die Rahmenbedingungen für klinische Prüfungen fest, die den Nutzen und die Sicherheit eines neuen Medikaments oder der Erweiterung des Anwendungsbereichs eines bekannten Medikaments vor der breiten Anwendung belegen müssen. Analog finden sich Regelungen für die Durchführung klinischer Prüfungen im Rahmen der Bewertung neuer Medizinprodukte im Gesetz über Medizinprodukte (MPG) und der zugehörigen Verordnung über klinische Prüfungen von Medizinprodukten (MPKPV). 2009 wurde eine grundlegende Überarbeitung des MPG verabschiedet, die u.a. die Regelungen zu klinischen Prüfungen mit denen des Arzneimittelrechts vereinheitlichen sollte. Hinsichtlich einiger datenschutzrelevanter Aspekte wurde dieses Ziel jedoch verfehlt, so dass auf diese gesondert in diesem Kapitel eingegangen wird.

Das Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz – AMG) wurde 2004 dahingehend grundlegend erweitert, dass es nicht mehr nur klinische Prüfungen im Rahmen einer kommerziell relevanten Zulassung regelt, sondern auch den Rechtsrahmen für wissenschaftlich motivierte Arzneimittelstudien bildet. Seit dieser 12. AMG-Novelle ist somit das Risiko der Probanden, welches mit der Anwendung eines neuen Arzneimittels oder dessen Anwendungserweiterung einhergeht, das entscheidende Kriterium für die Anwendbarkeit des Rechtsrahmens des AMG. Somit ist das AMG seit 2004 auch für einen Großteil der öffentlich geförderten klinischen Forschung relevant. Den immensen zusätzlichen Aufwänden, vom Studium und Verständnis der Regelungen bis hin zur Implementierung und regelmäßigen Überprüfung, stehen vor allem Sicherheits- und Qualitätsgewinne gegenüber.

Das AMG wurde seit 2004 mehrmals überarbeitet. Im Folgenden wird der Stand nach der 15. Novelle aus dem Jahr 2009 reflektiert, der allerdings hinsichtlich der Regelungen zum Datenschutz kaum Änderungen gegenüber der Fassung aus 2004 aufweist. Dieser Stand entspricht weitgehend auch einer nationalen Umsetzung der EU-Richtlinie 2001/20/EG. Auch für den Bereich des Arzneimittelrechts ist jedoch schon eine weitere europäische Vereinheitlichungsinitiative gestartet worden [21][14].

Aus Sicht des Datenschutzes sind insbesondere die Regelungen im AMG zur verpflichtenden Pseudonymisierung der erhobenen Daten im sechsten Ab-

14 Die neue „Verordnung des Europäischen Parlaments und des Rates über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG“ ist am 27.05.2014 als EU-Verordnung 536/2014 im Amtsblatt der Europäischen Union veröffentlicht worden. Die Verordnung ist am 16. Juni 2014 in Kraft getreten und gilt, abhängig von den bis dahin zu schaffenden Rahmenbedingungen, frühestens ab dem 28. Mai 2016. Sie wird dann die jeweils nationalen Regelungen zur Durchführung klinischer Arzneimittelstudien weitgehend ersetzen (s. http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014R0536).

schnitt zum „Schutz des Menschen bei der klinischen Prüfung“ sowie im vierten Abschnitt der zugehörigen GCP-Verordnung zu den Dokumentations- und Mitteilungspflichten von Interesse. Demnach sind die Daten innerhalb einer klinischen Prüfung insbesondere dem Sponsor nur in pseudonymisierter Form zur Verfügung zu stellen. Wenn die klinische Prüfung von einem industriellen Sponsor initiiert und verantwortet wird, so kann davon ausgegangen werden, dass dieser in aller Regel kein Interesse daran haben wird, die betroffenen Personen namentlich zu kennen. Somit setzt die Pseudonymisierungsverpflichtung lediglich das Prinzip der Datensparsamkeit aus dem Datenschutzrecht um. Gemäß § 40 Abs. 2a Satz 2 Nr. 1b AMG sind die Probanden einer klinischen Prüfung darüber zu informieren, dass die erhobenen Daten soweit erforderlich pseudonymisiert an den Sponsor oder eine von diesem beauftragte Stelle zum Zwecke der wissenschaftlichen Auswertung weitergegeben werden. Die Einwilligung in die pseudonymisierte Weitergabe der Daten erstreckt sich nach Satz 2 Nr. 1d auch auf die Verpflichtung der Meldung unerwünschter Ereignisse an den Sponsor, die zuständige Bundesoberbehörde und über diese an die hierfür eingerichtete europäische Datenbank. Entsprechende Hinweise darauf wie auch auf eingeschränkte (Satz 2 Nr. 3) oder fehlende Widerrufsmöglichkeiten (Satz 2 Nr. 2) sind in die Aufklärungs- bzw. Einwilligungsformulare aufzunehmen.

Die Regeln des AMG zur Pseudonymisierung sind so weit nachvollziehbar und entsprechen einer datenschutzgerechten Umsetzung. Im Sonderfall einer wissenschaftlich motivierten und initiierten Prüfung (Investigator Initiated Trial – IIT) ist jedoch zu beachten, dass Sponsor und Prüfer einer Studie identisch sein können. Für den Leiter der klinischen Prüfung wird dies regelmäßig gelten. Somit gibt es Konstellationen, in denen die personenbezogenen Daten für den Sponsor ohne weiteres jederzeit einsehbar oder ihm bekannt sind, da er zugleich diejenige Stelle ist, die die klinische Prüfung durchführt. Damit hat der Sponsor, soweit er gleichzeitig Prüfer ist, ohnehin jederzeit unbeschränkten direkten Zugriff auf die ihm gegenüber gem. § 40 Abs. 2a S. 2 Nr. 1b AMG grundsätzlich zu pseudonymisierenden Daten. In einem von der TMF in Auftrag gegebenen Gutachten kommt Dierks zu dem Schluss [22, S. B12], dass in diesen Fällen das Pseudonymisieren unter Betrachtung von Sinn und Zweck der gesetzlichen Vorschriften nicht erforderlich ist. Den Pflichten des Prüfers zur Übermittlung pseudonymisierter Daten an den Sponsor im Rahmen der Meldepflichten nach § 12 Abs. 4, 5 und 6 GCP V kommt aufgrund der Personenidentität von Prüfer und Sponsor bei IITs keine Bedeutung zu. Allerdings sind die Daten in IITs dann pseudonymisiert an den Sponsor zu übermitteln, wenn der Sponsor im Rahmen multizentrischer Studien nicht identisch mit der durchführenden Stelle bzw. dem konkreten Prüfer ist und somit auch nicht über Zugang zu den identifizierenden Daten der betroffenen Probanden verfügt.

Anders als im AMG finden sich in den Bestimmungen zu klinischen Prüfungen im MPG und in der MPKPV keine konkreten Vorschriften zu einer Pseudonymisierung von Daten. Die Umsetzung des datenschutzrechtlichen Prinzips

der Datensparsamkeit gebietet jedoch im Regelfall ebenfalls eine Pseudonymisierung der Daten, wenn diese außerhalb des Behandlungskontextes verarbeitet werden. Insofern wird die erstaunliche Unterschiedlichkeit der gesetzlichen Formulierungen diesbezüglich in der praktischen Umsetzung kaum Konsequenzen haben. Ein weiterer und für die Praxis relevanter Unterschied findet sich in den Vorgaben für die Einwilligungserklärungen: Die im AMG festgelegte Unwiderruflichkeit der Datenverarbeitung fehlt in den Bestimmungen des MPG. Vielmehr wird in § 20 Abs. 2 MPG explizit die jederzeit mögliche Widerrufbarkeit aufgeführt. Da dies dem datenschutzrechtlichen Standard entspricht, ergeben sich daraus im Vergleich zu Forschungsprojekten außerhalb des Regelungsbereichs von AMG und MPG keine Besonderheiten.

4.3.2 Gesundheitstelematik

Die langfristige Sammlung von Patientendaten auf nationaler Ebene, wie sie z.B. von den Kompetenznetzen in der Medizin zu wissenschaftlichen Zwecken seit jetzt über zehn Jahren betrieben wird, weist als Anwendungsfall viele Parallelen zu einigen der geplanten Anwendungen der im Aufbau befindlichen Telematikinfrastruktur auf Basis der elektronischen Gesundheitskarte (eGK) auf. So soll die eGK gemäß § 291a Abs. 3 Satz 1 Nr. 4 SGB V „... insbesondere das Erheben, Verarbeiten und Nutzen [...] von Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (elektronische Patientenakte) ...“ unterstützen. Demnach wäre eine elektronische Patientenakte (EPA) nach § 291a SGB V hinsichtlich der zu speichernden Daten, der vorgesehenen Dauer der Speicherung und des Verwendungszwecks z.T. durchaus vergleichbar mit dem Modell der Bereitstellung von Behandlungs- und Forschungsdaten in klinisch fokussierten Forschungsnetzen, wie es in der ersten Version der generischen Lösungen zum Datenschutz der TMF beschrieben wurde [1]. Im vorliegenden Konzept ist dieses Modell in Kapitel 5.1 zum Klinischen Modul weiterentwickelt worden. Aber auch die in § 291a Abs. 3 Satz 1 Nr. 5 SGB V vorgesehene Bereitstellung von Daten durch Versicherte selbst stellt einen für die Forschung zunehmend relevanten Anwendungsfall dar.

Bei diesen Überschneidungen der Ansätze und Interessen aus der Forschung mit denen aus der Versorgung liegt die Frage nach gemeinsamen Verwendungsmöglichkeiten einer einheitlichen Infrastruktur nahe. Nach § 291a Abs. 8 Satz 1 SGB V darf jedoch vom Inhaber der eGK nicht verlangt werden, einen Zugriff u.a. auf die Daten nach Abs. 3 Satz 1 „... zu anderen Zwecken als denen der Versorgung der Versicherten ...“ zu gestatten oder eine Gestattung mit ihm zu vereinbaren. In ihrem Gutachten kommen Roßnagel, Hornung und Jandt [11] entsprechend auch zu dem Schluss, dass eine rechtfertigende Einwilligung des Patienten in einen Zugriff auf die auf oder mittels der eGK gespeicherten Daten, die für die Nutzung zu Forschungszwecken notwendig wäre, jenseits der genannten Zwecke ausgeschlossen ist. Dies gilt ebenfalls für zusätzliche,

z.B. im Rahmen klinischer Studien erhobene Daten, wenn diese auf oder mit Hilfe der eGK gespeichert werden. Auch die von Patienten gemäß § 291a Abs. 3 Satz 1 Nr. 5 SGB V selbst in einem so genannten „Patientenfach" zur Verfügung gestellten Daten wären von diesem Verwendungsvorbehalt betroffen. Im Ergebnis ist damit eine Nutzung für die Forschung, auch als zusätzliche Funktion der Gesundheitskarte, nach geltendem Recht unzulässig.

Nach Roßnagel, Hornung und Jandt [11] ist ebenfalls die Nutzung der neuen Versichertennummer der eGK als identifizierendes Merkmal der Patienten im Forschungskontext unzulässig. Dies wäre für einrichtungsübergreifende Forschungsfragestellungen aufgrund des versicherungsunabhängigen und lebenslang gültigen Anteils der neuen Versichertennummer von Interesse und würde helfen, Patienten z.B. auch nach einem Namenswechsel eindeutig zuzuordnen. Nach Aussage der Gutachter ist das Verwendungsverbot unabhängig davon, ob die Versichertennummer direkt oder in nachvollziehbarer Weise umgeschlüsselt als Pseudonym genutzt wird, oder ob sogar nur eine Verwendung als identifizierendes Datum entsprechend der Vorgaben zum ID-Management in einem Forschungsverbund, wie in Kapitel 6.1.1.1 beschrieben und z.B. mit dem PID-Generator der TMF umsetzbar, geplant sei. Hintergrund dieser Einschätzung der Gutachter ist das bereits weiter vorne ausführlich erläuterte BSG-Urteil vom 10.12.2008 [12], welches die Verwendung von Sozialdaten aus dem zehnten Kapitel des SGB V zu nicht im SGB spezifizierten Zwecken auch bei Vorliegen einer Einwilligung ausschließt.

Nicht ausgeschlossen ist aber die Nutzung anderer Komponenten der im Aufbau befindlichen Telematikinfrastruktur, wie z.B. des Heilberufeausweises (HBA) zur einheitlichen und einrichtungsübergreifenden Authentifizierung der Nutzer zentraler IT-Infrastruktur-Komponenten der Forschungsnetze oder von Mehrwertdiensten (s. Glossar).

4.3.3 Eigentumsrecht bei Biomaterialien

Als weiterer relevanter Rechtsrahmen ist für biologische Proben das Sachenrecht nach § 854–1296 BGB zu berücksichtigen. Zwar gilt der menschliche Körper oder auch ein einzelnes Körperteil oder abgetrenntes Körpermaterial nicht als Sache im gesetzlichen Sinne. Für abgetrennte Körperteile oder Körpermaterialien wie Gewebe, Blut etc. trifft dies jedoch zunächst nur zu, wenn eine Wiedereingliederung geplant ist, wie z.B. bei einer Eigenblutspende oder einer Organtransplantation. Proben in Biomaterialbanken für die Forschung sind jedoch durchweg Körpermaterialien, die eindeutig ohne Absicht und Möglichkeit der Wiedereingliederung entnommen worden sind. Damit sind sie als Sachen im Sinne des § 90 BGB einzuordnen [23, S. 32].

Das auf das Sachenrecht zurückgehende Eigentumsrecht steht grundsätzlich und ohne weitere Vereinbarung den Spendern zu. Dabei wird das Eigentumsrecht an den Proben vom allgemeinen Persönlichkeitsrecht überlagert, wobei

die Intensität dieser Überlagerung davon abhängt, in welchem Umfang Rückschlüsse vom Körpermaterial auf dessen ehemaligen Träger und seine Person gezogen werden können. Nur wenn solche Rückschlüsse nicht mehr möglich sind, wäre das allgemeine Persönlichkeitsrecht bedeutungslos. Das im Regelfall anzunehmende Persönlichkeitsrecht, wie auch das in Verbindung damit stehende Widerrufsrecht der Probanden schließen eine implizite Eigentumsübertragung im Rahmen der Einwilligung in die Teilnahme an einem Forschungsprojekt üblicherweise aus [23]. Eine explizite Eigentumsübertragung ist aber nach allgemeiner Auffassung möglich, auch wenn die Persönlichkeitsrechte an der Probe nicht übertragbar sind und damit notwendigerweise von der Eigentumsübertragung unberührt bleiben [5, S. 118]. Wenn ein Verwertungsbedarf in Bezug auf die Proben nicht ausgeschlossen werden kann, sollten die Probanden entsprechend explizit um eine Eigentumsübertragung gebeten werden. Als weiterführende Lektüre zu diesem Themenkomplex wird auf das im Auftrag der TMF erstellte Rechtsgutachten von Simon und Mitarbeitern verwiesen, welches als Band 2 der Schriftenreihe der TMF veröffentlicht wurde [23].

4.3.4 Abgleich mit externen Datenbeständen

Gerade in epidemiologischen Forschungsprojekten kann ein berechtigtes Interesse an Datenübermittlungen von beispielsweise Einwohnermelde-, Gesundheits- oder Standesämtern bestehen. Die gesetzlichen Grundlagen für die Übermittlung von Daten aus Melderegistern stehen typischerweise in den Meldegesetzen der Länder. So erlaubt z.B. § 31 Abs. 1 des Meldegesetzes für Rheinland-Pfalz den Meldebehörden die Übermittlung bestimmter Daten an andere Behörden oder öffentliche Stellen, soweit dies zur Erfüllung von Aufgaben erforderlich ist, die in ihrer Zuständigkeit oder der der empfangenden Stelle liegen. Regelungen für die Standesämter finden sich hingegen im Personenstandsgesetz (PStG). Für einige Forschungsprojekte ist auch eine genaue Kenntnis der Todesursachen verstorbener Patienten notwendig. Solche Daten können in bestimmten Fällen von den Gesundheitsämtern angefordert werden. Den gesetzlichen Rahmen für solche Informationsübermittlungen spannen die Gesundheitsdienstgesetze der Länder auf. Eine weitere relevante Datenquelle können die Krebsregister auf Landesebene sein, für die in den Landeskrebsregistergesetzen die Bedingungen für eine Datenweitergabe zu Forschungszwecken festgehalten sind.

4.4 Patientenrechte

4.4.1 Auskunftsrechte

Jeder Proband hat nach § 34 (1) BDSG ein grundsätzliches Recht auf Auskunft über die von ihm gespeicherten personenbezogenen Daten, also auch über abgeleitete oder aus Biomaterialien gewonnene Daten. Zu dieser Auskunfts-

pflicht gibt es in § 33 (2) BDSG aufgezählte Ausnahmen, wie etwa ein unverhältnismäßiger Aufwand, die Geheimhaltungspflicht aufgrund einer Rechtsvorschrift oder wegen des überwiegenden rechtlichen Interesses eines Dritten, die Gefährdung der öffentlichen Sicherheit oder Ordnung oder eine erhebliche Gefährdung der Geschäftszwecke der verantwortlichen Stelle, die jedoch in der Regel auf die hier behandelten Daten- und Probensammlungen der Forschung nicht zutreffen. Die Möglichkeit der Auskunft besteht nur, solange die Daten nicht anonymisiert wurden. Korrespondierend zu den Auskunftsrechten besteht nach § 35 BDSG das Recht der Probanden auf Berichtigung, Löschung oder Sperrung ihrer Daten.

4.4.2 Recht auf Wissen und Nichtwissen

An den Ergebnissen medizinischer Forschung können Probanden ein berechtigtes Mitteilungsinteresse haben, insbesondere dann, wenn es sich um individuelle Untersuchungsergebnisse mit medizinischer Relevanz handelt. Die Möglichkeit der Entstehung solcher Ergebnisse kann gerade bei Nutzung umfangreicher Daten- und Probensammlungen immer seltener von vornherein ausgeschlossen werden. Vor diesem Hintergrund sollten die Probanden im Vorfeld über mögliche Untersuchungsergebnisse aufgeklärt und mit ihnen eine entsprechende Auskunftsregelung vereinbart werden. Dabei ist allerdings auch zu berücksichtigen, dass Probanden bestimmte Untersuchungsergebnisse möglicherweise nicht mitgeteilt bekommen möchten. Dies kann z.B. auf Ergebnisse aus genetischen Untersuchungen oder andere Befunde mit prädiktivem Charakter zutreffen. Auch diesem Recht auf Nichtwissen ist in entsprechenden Vereinbarungen Rechnung zu tragen [vgl. 24; 25]. In diesem Zusammenhang sind Probanden zudem darauf hinzuweisen, dass sie ihnen bekannte Untersuchungsergebnisse ggf. auch Versicherungen oder Arbeitgebern mitteilen müssen. Zum anderen können Ergebnisse aus genetischen Untersuchungen auch eine Relevanz für Angehörige des Probanden aufweisen, so dass deren Recht auf Nichtwissen auch zu berücksichtigen ist. Sollte ein Proband darauf bestehen, über die Ergebnisse der genetischen Untersuchungen informiert zu werden, so kann ihm das aufgrund seines informationellen Selbstbestimmungsrechts nicht versagt werden. Er kann jedoch dann selbst in den Konflikt geraten, einerseits Angehörige darüber informieren zu wollen, dass relevante Informationen aus genetischen Untersuchungen vorhanden sind, andererseits aber auch deren Recht auf Nichtwissen respektieren zu müssen. Auf eine solche mögliche Konfliktsituation sollten Probanden daher im Vorfeld hingewiesen werden [weitere Informationen hierzu in: 5, S. 78].

Bei der Festlegung eines Standardverfahrens, von welchem im Rahmen abgestufter Einwilligungserklärungen in vordefinierter Form auch abgewichen werden kann, sollte berücksichtigt werden, dass gerade viele Zufallsbefunde aus genetischen oder anderen Untersuchungen bei geringer tatsächlicher Relevanz für die Probanden doch gleichzeitig auch erhebliches Verunsicherungs-

potenzial besitzen können. Zudem ist der Aufwand der Informierung der Probanden nicht zu unterschätzen, da zum einen möglicherweise auch Beratungskompetenz mit zur Verfügung gestellt und zum anderen die notwendige Depseudonymisierung mit allen damit verbundenen Komplikationen geregelt werden muss. Hinsichtlich der Depseudonymisierung ist an ggf. notwendige Entbindungen von der Schweigepflicht zu denken oder es müssen technische und organisatorische Verfahren implementiert werden, die sicherstellen, dass nur der behandelnde Arzt den Untersuchungsbefund in depseudonymisierter Form erhält.

Vor dem Hintergrund der genannten Aufwände und der möglicherweise in vielen Fällen geringen Relevanz der Mitteilung von Zufallsbefunden kann ein Forschungsprojekt auch vorsehen, dass die Probanden mit der Einwilligungserklärung auf ein Mitteilungsrecht zunächst verzichten. Dies kann auch zur Bedingung einer Teilnahme am Forschungsprojekt gemacht werden [14]. Allerdings ist zu beachten, dass Probanden diese Vereinbarung auch widerrufen können und ihnen das Auskunftsrecht dann zu einem späteren Zeitpunkt doch zusteht. Ein unwiderruflicher Verzicht auf Mitteilung von Untersuchungsergebnissen kann nicht mit den Probanden vereinbart werden.

Ein vereinbarter Verzicht auf die Mitteilung von Ergebnissen kann in bestimmten Fällen die spätere Rekrutierung von Probanden einschränken. Dies kann z.B. der Fall sein, wenn für eine Präventionsstudie überwiegend oder ausschließlich Patienten rekrutiert werden sollen, die bestimmte Risikofaktoren aufweisen und der vereinbarte Mitteilungsverzicht impliziert, dass der Proband über das Vorhandensein eines solchen Risikofaktors nicht informiert wird.

Von den Auskunftsrechten der Patienten sind u.U. ärztlich begründete Mitteilungspflichten der Forscher zu unterscheiden. Diese beziehen sich z.B. auf wichtige medizinische Befunde mit unmittelbaren Konsequenzen für eine weitere Behandlung oder Diagnostik. Der hierfür nötige Regelungsumfang entspricht weitgehend jenem für die Auskunftsrechte der Probanden. Die entsprechenden Vereinbarungen können somit analog formuliert werden. Grundsätzlich ist zu beachten, dass alle genannten Auskunftsrechte der Patienten und Mitteilungspflichten der Forscher sich nur auf Daten beziehen, die nicht anonymisiert wurden [5, S. 132].

4.4.3 Einbeziehung von Ethikkommissionen

Die Berücksichtigung der vorliegenden Empfehlungen zur datenschutzgerechten Umsetzung medizinischer Forschungsprojekte kann und soll die sorgfältige Beratung und Prüfung eines Forschungsprojekts in jedem Einzelfall durch eine oder mehrere Ethikkommissionen nicht ersetzen. Eine berufsrechtliche Pflicht, sich durch eine Ethikkommission beraten zu lassen, ergibt sich aus den Regelungen der Berufsordnungen. Dies gilt immer dann, wenn im Rah-

men eines Forschungsprojekts in die psychische oder körperliche Integrität eines Menschen eingegriffen wird oder personenbezogene Proben oder Daten verwendet werden (§ 15 MBO). Für Forschungsvorhaben im Anwendungsbereich des Arzneimittelrechts ist eine Prüfung gemäß § 40 (1) AMG verpflichtend, gleiches gilt für nach Medizinproduktegesetz geregelte klinische Prüfungen (§ 20 [7] MPG). Gleichwohl soll der hier vorgelegte konzeptionelle Rahmen die Überprüfung von Forschungsprojekten in Bezug auf datenschutzrechtliche Fragen durch Ethikkommissionen vereinfachen und verbessern helfen. Gerade die Abstimmung und Prüfung einrichtungsübergreifender und auf Langfristigkeit angelegter Datensammlungen mit ihren entsprechend aufwändigen Schutzprinzipien wird von einem allseits anerkannten Bezugsrahmen profitieren und beschleunigt werden.

Die Prüfung datenschutzrechtlicher Aspekte betrifft zudem nur einen Teil des Aufgabenspektrums der Ethikkommissionen. Ihr Auftrag umfasst die Prüfung der medizinischen Forschung am Menschen aus ethischer, rechtlicher und sozialer Sicht und geht wesentlich auf die Deklaration von Helsinki zurück [26]. So ist beispielsweise bei interventionellen Studien das Studiendesign daraufhin zu prüfen, ob alle schonenderen oder weniger riskanten Untersuchungsmöglichkeiten sorgfältig erwogen und begründet ausgeschlossen wurden. Andererseits ist auch abzuklären, ob das gewählte Studiendesign samt vorgesehener Stichprobengröße überhaupt zu Ergebnissen führen kann, die das Risiko für jeden einzelnen Patienten rechtfertigen. Schließlich sind die Aufklärungs- und Einwilligungsformulare zu begutachten, was wiederum auch datenschutzrechtliche Aspekte betrifft.

4.5 Ebenen des Datenschutzrechts und der Datenschutzaufsicht

Viele Forscher stehen zu Beginn der datenschutzrechtlichen Klärung ihres Projekts vor zwei Fragen: Welches Datenschutzgesetz gilt für mein Projekt und welcher Datenschutzbeauftragte ist mein Ansprechpartner? Ein Blick in das virtuelle Datenschutzbüro für Deutschland, angeboten vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), zeigt, dass es neben dem Bundesdatenschutzbeauftragten und dem Bundesdatenschutzgesetz auch Regelungen und Ansprechpartner für jedes der 16 Bundesländer in Deutschland gibt[15]. Zusätzlich gibt es in öffentlichen Einrichtungen im Regelfall auch noch einen behördlichen und in privat getragenen Einrichtungen ab einer bestimmten Größe einen betrieblichen Datenschutzbeauftragten, der als Ansprechpartner in Frage käme. Wo also anfangen?

Das im vorliegenden Text hauptsächlich referierte Bundesdatenschutzgesetz gilt nach § 1 (2) BDSG für öffentliche Stellen des Bundes und nicht-öffentliche

15 siehe http://www.datenschutz.de/recht/gesetze/

Stellen, also Einrichtungen in privater Trägerschaft. Eingeschränkt gilt es auch für bestimmte Aufgabenbereiche einiger weniger öffentlicher Stellen der Länder. Entsprechend sind die Bestimmungen des Bundesdatenschutzgesetzes in Krankenhäusern in privater Trägerschaft anzuwenden, in Universitätskliniken im Regelfall jedoch nicht, da diese überwiegend öffentliche Einrichtungen der Länder sind. Die datenschutzrechtlichen Belange der öffentlichen Stellen der Länder sind in den Landesdatenschutzgesetzen geregelt[16, 17].

Sowohl auf Landes- wie auf Bundesebene sind in den Datenschutzgesetzen an vielen Stellen die Prinzipien der Europäischen Richtlinie zum Datenschutz 95/46/EG von 1995 umgesetzt. Nicht nur, aber auch aus diesem Grunde sind die Ausführungen an vielen Stellen schon weitgehend harmonisiert, so dass tatsächlich häufig das Bundesdatenschutzgesetz stellvertretend für die Landesdatenschutzgesetze zitiert werden kann. Insofern wäre es auch nicht gerechtfertigt, in Bezug auf das Datenschutzrecht in Deutschland von einem „Flickenteppich" zu sprechen. Unübersichtlich wird die Lage allerdings insofern als das Datenschutzrecht nur subsidiär zu anderen Gesetzen anzuwenden ist. Namentlich die Landeskrankenhausgesetze führen daher effektiv zu unterschiedlichen datenschutzrechtlichen Bedingungen in den Ländern, gerade auch für die Sekundärnutzung klinischer Daten, wie bereits weiter oben ausgeführt. Einen ersten Überblick hierzu haben Schütze und Oemig ausgearbeitet [27], der allerdings z.B. in Bezug auf das Berliner Krankenhausgesetz schon veraltet ist. Aber auch die Landesdatenschutzgesetze unterscheiden sich doch so weit voneinander, dass für ein konkretes Projekt ggf. das relevante Landesrecht detailliert geprüft werden muss. In größeren Projekten mit der Beteiligung mehrerer öffentlicher Einrichtungen wird die Prüfung heute im Regelfall die Gesetze mehrerer Länder umfassen müssen. Die Mühseligkeit eines solchen Unterfangens zeigt sich u.a. darin, dass auch die Datenschützer selbst in ihren Veröffentlichungen eine genaue Prüfung der landesdatenschutzrechtlichen Besonderheiten mitunter vermeiden [z.B. 28, s. Fußnote 26 auf S. 26].

Als direkter Ansprechpartner für ein konkretes Forschungsprojekt kommt der Bundesbeauftragte für den Datenschutz eher selten in Betracht. Dabei ist es unerheblich, ob private oder öffentliche Stellen in das Projekt involviert sind. Ihm obliegt nach § 24 BDSG im Wesentlichen die Aufsicht über die öffentlichen Stellen des Bundes. Die Aufsicht über private Stellen und die öffentlichen Stellen der Länder ist hingegen auf Länderebene geregelt. Für die öffentlichen

16 Spezifische Regelungen der Kirchen zum Datenschutz sind hier nicht weiter berücksichtigt

17 In einigen Landesdatenschutzgesetzen finden sich Hinweise auf die teilweise Anwendbarkeit des BDSG auch für Einrichtungen in öffentlicher Trägerschaft, wenn diese im Wettbewerb mit privat getragenen Einrichtungen stehen, so z.B. in § 3 BayDSG. Eine Teilnahme am Wettbewerb um Behandlungsverhältnisse kann für öffentlich getragene Krankenhäuser im Regelfall angenommen werden. Eine ausführliche und vergleichende Darstellung der landesdatenschutzrechtlichen Rahmenbedingungen für die Sekundärnutzung klinischer Daten findet sich in einem von der TMF in Auftrag gegebenen und ebenfalls in der TMF-Schriftenreihe veröffentlichten Rechtsgutachten.

Stellen ist in den Landesdatenschutzgesetzen die Zuständigkeit der Landesbeauftragten für den Datenschutz (LfD) festgelegt. Die Aufsicht über den privaten Bereich lag bis vor kurzem in den meisten Ländern bei nachgeordneten Behörden der Innenministerien der Länder, z.B. Regierungspräsidien. Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 9. März 2010 festgestellt, dass diese Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt sind und damit das Erfordernis gemäß Richtlinie 95/46/EG, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit" wahrnehmen, nicht umgesetzt ist [29]. Dieses Urteil hatte in den meisten Bundesländern eine Neuordnung der Datenschutzaufsicht für den privaten Bereich zur Folge, die im Ergebnis in allen Bundesländern bis auf Bayern zu einer erweiterten Zuständigkeit der Landesdatenschutzbeauftragten geführt hat. In Bayern ist das Bayerische Landesamt für den Datenschutz die zuständige Kontrollstelle für nicht-öffentliche Stellen.

Direkter und erster Ansprechpartner könnte in öffentlichen Institutionen der behördliche und in privat getragenen Einrichtungen ab einer gewissen Mindestgröße der betriebliche Datenschutzbeauftragte sein. Die frühzeitige Besprechung von Forschungsvorhaben mit diesen lokalen Ansprechpartnern kann grundsätzlich nur empfohlen werden. Allerdings ist es wichtig zu verstehen, wann darüber hinaus auch die Abstimmung mit den zuständigen Landesdatenschutzbeauftragten angestrebt werden sollte. Die Zuständigkeiten von behördlichem bzw. betrieblichem Datenschutzbeauftragten und dem Landesbeauftragten für den Datenschutz sowie deren Verhältnis untereinander werden im Folgenden exemplarisch für öffentliche Einrichtungen in NRW dargestellt. Diese Ausführungen sollen das komplexe Zusammenspiel der Zuständigkeiten beispielhaft veranschaulichen. Sie lassen sich jedoch nicht direkt auf andere Bundesländer übertragen. Eine Untersuchung der Gegebenheiten in allen Bundesländern würde den Rahmen dieses Leitfadens sprengen. Die TMF plant zu diesem Thema ein Rechtsgutachten einzuholen, welches dann zu einem späteren Zeitpunkt auf der Website der TMF zur Verfügung gestellt wird[18].

Die jeweiligen Aufgaben und Zuständigkeiten sind im Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) festgelegt. Der behördliche Datenschutzbeauftragte hat nach § 32a DSG NRW die Sicherstellung des Datenschutzes in der Einrichtung zu unterstützen. Konkret hat er hierfür insbesondere gemäß § 8 DSG NRW ein lokales Verzeichnis automatisierter Verfahren zur Verarbeitung personenbezogener Daten (Verfahrensverzeichnis) zu führen und gemäß § 32a Absatz 1 Satz 7 DSG NRW Vorabkontrollen durchzuführen. Die Aufgaben und Befugnisse des Landesbeauftragten für Datenschutz und Informationsfreiheit sind in § 22 DSG NRW geregelt. Der Landesbeauftragte ist Aufsichts- und Kontrollbehörde für Datenschutzfragen in NRW. Gemäß § 25 DSG NRW hat jede

18 siehe www.tmf-ev.de/produkte

Person das Recht, sich unmittelbar an ihn zu wenden, wenn er bzw. sie der Ansicht ist, dass gegen datenschutzrechtliche Vorschriften verstoßen worden ist oder ein solcher Verstoß bevorsteht. Der Landesbeauftragte ist zudem gemäß § 4a Absatz 1 Satz 5 DSG NRW über die Errichtung von Verbunddateien und gemäß § 9 Absatz 2 Satz 5 DSG NRW über die Einrichtung automatisierter Abruf- und Übermittlungsverfahren zu unterrichten.

Anfang 2012 hat die Europäische Kommission den Entwurf einer europäischen Datenschutzgrundverordnung (DGVO) vorgestellt [6]. Anders als bei der bisherigen Richtlinie zum Datenschutz, die von den einzelnen Ländern der EU in einem jeweils individuellen Verfahren in nationales Recht umzusetzen war, würde eine solche Verordnung auf europäischer Ebene direkt nationales Recht ersetzen. Damit wäre in weiten Teilen auch eine innerdeutsche Harmonisierung des Datenschutzrechts, sowohl für private wie für öffentliche Stellen, erreicht, was grundsätzlich positiv zu bewerten ist. Zudem enthält der Entwurf in Artikel 83 Regelungen für die Forschung, die eine lokale Nutzung von Daten, vorranging und wenn möglich anonymisiert oder pseudonymisiert, auch ohne Einwilligungserfordernis erlauben würden. Dies könnte zumindest für lokale oder monozentrische Forschungsprojekte eine große Erleichterung bedeuten.

Allerdings wird dieser Entwurf aktuell auf europäischer Ebene und in den Ländern umfassend kommentiert, so dass noch mit einer Reihe von Änderungen zu rechnen ist. Zudem enthält der Entwurf zahlreiche Ermächtigungsklauseln für die Europäische Kommission, delegierte Rechtsakte in Form von Ausführungs- und Konkretisierungsbestimmungen zu erlassen, so auch zu Artikel 83 DGVO. Eine abschließende Bewertung dieser europäischen Gesetzgebungsinitiative ist daher noch nicht möglich.

4.6 Grundprinzipien datenschutzgerechter Lösungen

Der hier dargelegte konzeptuelle Rahmen für datenschutzgerechte Lösungen in der medizinischen Forschung basiert auf einigen elementaren Prinzipien, die im Folgenden zusammengefasst dargestellt sind. Auf ausführlichere Darstellungen zu den einzelnen Prinzipien in anderen Kapiteln wird jeweils verwiesen.

Das **Risiko einer unerlaubten Reidentifizierung** sollte so weitgehend wie möglich und nötig ausgeschlossen werden. Weitere Hinweise zur Verhältnismäßigkeit unterschiedlicher Lösungsansätze finden sich in Kapitel 6.7.

Das Prinzip der **informationellen Gewaltenteilung** sieht vor, dass, wenn möglich und nötig, die gespeicherten identifizierenden Personendaten von den medizinischen Daten getrennt aufbewahrt und verwaltet werden. Im Maximalfall sind hierfür getrennte Institutionen verantwortlich, die keiner gemeinsamen Weisungsbefugnis unterstehen. Zudem kann auch die Verwal-

tung eines Zuordnungsschlüssels in die eigenständige Verwaltung eines unabhängigen Treuhänders gegeben werden. Eine ausführliche Darstellung bietet Kapitel 6.1.

Das Prinzip **sicherer Pseudonyme** ergänzt das Prinzip der informationellen Gewaltenteilung. Pseudonyme sind langfristig sichere, kryptographisch erzeugte Identifikatoren, die nur entlang vorgesehener und rechtmäßiger Verarbeitungs- und Genehmigungsprozeduren eine Reidentifizierung von Probanden ermöglichen. Weitere Informationen sind in Kapitel 6.1 zum ID-Management zu finden.

Das Prinzip der sorgfältigen **Abwägung zwischen Anonymisierung und Pseudonymisierung** erfordert eine genaue Kenntnis der Anwendungsfälle und Nutzungsszenarien. Das Gros der hier dargestellten Anwendungsfälle erfordert eine langfristige pseudonymisierte Speicherung medizinischer Daten, was neben einer Rechtsgrundlage der strikten organisatorischen Einhegung samt effektiver Zugangskontrolle bedarf. Andererseits ist bei anonymisierten Daten immer zu beachten, wie sicher und dauerhaft eine Reidentifizierung ausgeschlossen werden kann. Eine Verwendung solcher Daten in Public-Use-Files setzt eine nachweisbare Anonymisierung voraus, wie sie z.B. das Konzept der k-Anonymisierung (Erläuterung im Glossar) bietet. Genauere Darstellungen beinhalten das Kapitel 5.3 zu Forschungsdatenbanken und das Kapitel 6.1 zum ID-Management.

Das Prinzip **rechtlich klar und transparent geregelter Verantwortlichkeiten** wird durch eine rechtsfähige Organisationsform eines Forschungsverbunds unterstützt.

Das Prinzip der **Kombination technischer und organisatorischer Sicherheitsmaßnahmen** wird durch parallele und ergänzende Anwendung technischer Vorkehrungen wie z.B. Zugriffsbeschränkungen, kryptographische Transformationen, Logging etc. und organisatorischer Regelungen wie z.B. Standard Operating Procedures, klare Verantwortlichkeiten, Vier-Augen-Prinzip bei wichtigen Entscheidungen usw. umgesetzt und ist für einen hohen Sicherheitsstandard im Regelfall unerlässlich.

Das Prinzip **redundanter Absicherung** führt zu einem Schutz der Daten auch dann, wenn eine Sicherungskomponente ausfällt. Dies kann z.B. ein kurzfristig unsicher gewordenes kryptographisches oder technisches Verfahren sein oder eine unerlaubte Umgehung organisatorischer Regelungen. So wird z.B. empfohlen, medizinische und identifizierende Daten nicht gemeinsam über öffentliche Netze wie das Internet zu übertragen und zusätzlich für eine Verschlüsselung der Inhalte auf dem aktuellen Stand der Technik zu sorgen.

Das Prinzip **möglichst einfacher und ökonomischer Lösungen** setzt eine sorgfältige Analyse des konkreten Anwendungsfalls voraus, so dass eine dem Schutzbedarf angepasste und den Kriterien der Verhältnismäßigkeit genügende Implementierung realisiert werden kann. Eine detaillierte Aufstellung re-

levanter Kriterien für eine Anpassung des Sicherheitsaufwands findet sich in Kapitel 6.7.

Das Prinzip der **bestmöglichen Nutzung** aufwändig und womöglich mit persönlichem Risikoeinsatz der beteiligten Probanden erhobener Daten ist einerseits ein ethisches Gebot, dem jedoch andererseits durch das Prinzip der **informierten Einwilligung** Grenzen gesetzt werden. Die Komplexität des hier vorgestellten konzeptuellen Rahmens für datenschutzgerechte Lösungen resultiert ganz wesentlich aus dem Anliegen, auf Langfristigkeit angelegte, pseudonymisierte Datensammlungen zu ermöglichen, die vergleichsweise zweckoffen für die Forschung genutzt werden können, ohne dass Patienten oder Probanden mit ihrer Einwilligung ein unabsehbares Risiko in Bezug auf den ethischen und datenschutzgerechten Umgang mit ihren Daten eingehen.

Zu dem Prinzip der **informationellen Selbstbestimmung** gehört sowohl das Recht auf Wissen als auch das Recht auf Nichtwissen. Wie sichergestellt werden kann, dass Patienten über ihre Daten und Ergebnisse informiert werden können, ohne ihnen dabei nicht gewünschte Informationen aufzudrängen, ist den einzelnen Kapiteln zu den verschiedenen Anwendungsfällen mit ihren jeweiligen Lösungskonzepten zu entnehmen. Jede Diagnostik, die genetische Informationen offenbart, führt in diesem Zusammenhang allerdings zu komplexen Anforderungen, insbesondere hinsichtlich der informationellen Selbstbestimmung der Angehörigen eines Probanden. Hier ist eine entsprechend detaillierte Analyse möglicher Konflikte unerlässlich und jede einmal gefundene Lösung muss eventuell später an neue Rahmenbedingungen angepasst werden.

Die **Vermeidung von Rollenkonflikten** ist als wichtiges Prinzip bei der Festlegung der Rollen und Rechte in einem Forschungsverbund zu berücksichtigen. Eine genaue Prüfung auf mögliche Rollenkonflikte ist in jedem Forschungsvorhaben unerlässlich, insbesondere sollte jede Umgehung des Prinzips der informationellen Gewaltenteilung ausgeschlossen werden. Weitere Hinweise finden sich in Kapitel 6.2.3.

5 Module des Datenschutzkonzepts

Das generische Datenschutzkonzept für medizinische Forschungsverbünde ist modular aufgebaut. Die Module unterscheiden sich durch unterschiedliche Rahmenbedingungen und Vorgehensweisen und passen somit zu unterschiedlichen wissenschaftlichen Fragestellungen. Da ein Forschungsverbund oft viele verschiedenartige Forschungsprojekte vereinigt, dienen die Module und die zentralen Infrastruktur-Komponenten als Bausteine, aus denen das Datenschutzkonzept des Verbundes zusammengesetzt werden kann.

Ein medizinischer Forschungsverbund besteht aus bis zu vier Modulen:

- **Klinisches Modul** – dieses dient der Gewinnung von Forschungsdaten aus dem direkten Behandlungszusammenhang; ferner können hier auch einfache oder informelle Forschungsprojekte wie Beobachtungsstudien oder Benchmarkingprojekte durchgeführt werden. Der wissenschaftliche Austausch von behandelnden Ärzten mit führenden Experten im direkten Interesse des Patienten wird gefördert. Der Online-Zugriff auf die Daten während der Behandlung ist notwendig.
- **Studienmodul** – hier werden klinische Studien durchgeführt, die auch den besonderen Regularien des Arzneimittelgesetzes (AMG) oder Medizinproduktegesetzes (MPG) unterliegen können.
- **Forschungsmodul** – in diesem werden besonders qualitätsgesicherte Daten für langfristige Forschungsprojekte zusammengeführt und vorgehalten, die für die Behandlung des einzelnen Patienten keine direkte Rele-

vanz haben und daher aus dem Behandlungskontext nicht zugänglich sein müssen; Beispiele hierfür sind epidemiologische Register.

- **Biobankenmodul** – dieses dient der Sammlung und Verwaltung von Biomaterialien (Proben und daraus gewonnene Materialien) für Forschungszwecke, insbesondere für die Erforschung molekulargenetischer Aspekte einer Erkrankung wie Fragestellungen der genetischen Epidemiologie.

Die Module unterscheiden sich in ihrer Zweckbestimmung und ihrer Datenprozessierung und unterliegen unterschiedlichen rechtlichen Rahmenbedingungen. Jedes dieser Module enthält eine spezifische zentrale Datenbank, in manchen Fällen auch mehrere gleichartige. Die Module werden durch zentrale Infrastruktur-Komponenten zum Identitätsmanagement für Patienten sowie zum Rechtemanagement für Teilnehmer des Forschungsverbundes ergänzt.

In diesem Kapitel werden die Module einzeln beschrieben, ihre unterschiedlichen Rahmenbedingungen und Verfahren spezifiziert und Anleitungen für das Datenschutzkonzept von „einfachen“ Forschungsverbünden gegeben, die im Wesentlichen nur aus einem Modul bestehen (s.a. Abb. 6).

Kombinationsvarianten der unterschiedlichen Module wie auch zentrale Aspekte des Identitäts- und Rechtemanagements in einem Forschungsverbund sind dann Gegenstand des folgenden Kapitels 6.

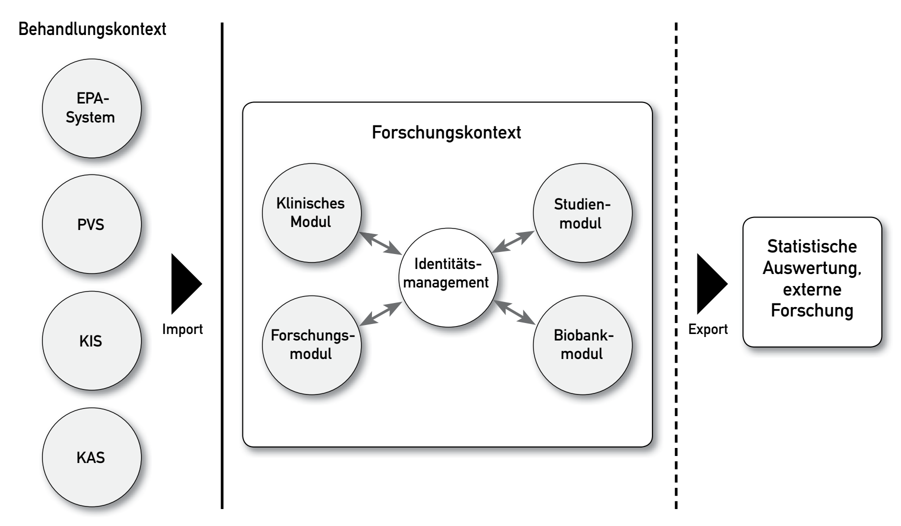


Abb. 6 Module eines medizinischen Forschungsverbunds; neben dem Identitätsmanagement sind auch andere zentrale Dienste nötig, etwa Rechtemanagement oder Datenqualitätsmanagement.

5.1 Klinisches Modul

Das klinische Modul stellt die Adaption des Modells A des bisherigen generischen TMF-Datenschutzkonzepts dar; die Einordnung in die neue Struktur ist in Kapitel 6.1.7 beschrieben.

Die Bezeichnung als „Klinisches Modul“ folgt der Bezeichnung „klinisch-(wissenschaftliches) Forschungsnetz“ aus dem bisherigen Datenschutzkonzept. Sie soll darauf hindeuten, dass in diesem Modul klinische Forschung betrieben wird, also im Wesentlichen Forschung direkt am Patienten in engem Versorgungsbezug[19]. Die spezialgesetzlich geregelten klinischen Studien werden wegen ihrer besonderen gesetzlichen und methodischen Rahmenbedingungen nicht hier, sondern in das Studienmodul eingeordnet, siehe Kapitel 5.2.

5.1.1 Zweck und Anwendungsbereich

Das Ziel des Klinischen Moduls ist die Ableitung und Bereitstellung von Forschungsdaten aus dem normalen Behandlungsgeschehen, in erster Linie ohne zusätzliche erhebliche Intervention zu Forschungszwecken. Dieses Ziel wird beispielsweise im Rahmen von Beobachtungsstudien, der Dokumentation von Heilversuchen oder bei gesundheitsökonomischen Studien realisiert und erfordert dazu eine klinisch fokussierte Vernetzung. Die Einsetzbarkeit des Klinischen Moduls ergibt sich insbesondere bei der Erforschung von Erkrankungen, die so selten sind oder deren Behandlung so komplex ist, dass sie die Leistungsfähigkeit von einzelnen Regelversorgungszentren überfordert. In diesen Fällen ist die enge Kooperation und Kommunikation spezialisierter Zentren unverzichtbare Voraussetzung sowohl für die effektive Behandlung als auch für aussagekräftige Forschungsergebnisse.

Patienten mit chronischen, seltenen oder besonders schweren Erkrankungen werden oft sowohl von ihren Hausärzten als auch zusammen mit breit gefächerten spezialisierten klinischen Zentren, wie z.B. Spezialkliniken, spezialisierten niedergelassenen Ärzten, sogenannten Referenzlaboren oder Referenzpathologien, betreut. Durch das Hinzuziehen spezialisierter und im jeweiligen Fachgebiet besonders erfahrener Behandlungsteams soll eine höhere Diagnostik- und Therapiequalität erreicht werden, als dies alleine im Bereich der Regelversorgung möglich ist. Solche Kooperationsstrukturen aufoder auszubauen, ist Aufgabe z.B. der Kompetenznetze in der Medizin oder der Netze für seltene Erkrankungen.

19 Die ebenfalls diskutierte Bezeichnung als „Versorgungsmodul“ wurde – obwohl in einigen Forschungsverbünden im Gebrauch – verworfen, da die Verwechslungsgefahr mit den Strukturen der direkten Krankenversorgung zu groß ist.

Wegen der fundierten Erfahrung und des hier gebündelten Sachverstandes tragen die spezialisierten Zentren besondere Verantwortung sowohl für die Versorgung nach aktuellem Stand des Wissens als auch in der Weiterentwicklung und Evaluation von diagnostischen und therapeutischen Verfahren. Im Bereich der Versorgung fallen ihnen oft Aufgaben in der Beratung von Patienten (Zweitmeinung) wie auch von Ärzten zu, die an der Regelversorgung beteiligt sind. So soll ein vom Zentrum initiierter Behandlungspfad oder Therapieplan im klinischen Alltag zumindest teilweise auch von nicht spezialisierten Behandlungsteams heimatnah und kostengünstig durchgeführt werden können. Bei Änderungen im Krankheitsverlauf oder zu vorher festgelegten Zeitpunkten erfolgt die Wiedervorstellung der Patienten im spezialisierten Zentrum.

Auch die spezialisierten klinischen Zentren greifen bei ihrer Arbeit wiederum auf weitere Spezialisten zurück. So werden beispielsweise besondere Laboruntersuchungen oft nicht in allen Zentren durchgeführt, selbst wenn hier auf Grund der Behandlung bestimmter Patientenkollektive die Ergebnisse dieser Methoden benötigt werden. Die Durchführung hochspezieller Analysen erfolgt ebenso oft in einem wiederum hierfür spezialisierten Zentrum, das die Anforderungen mehrerer klinischer Zentren bündelt und bearbeitet. Die Behandlung der oben genannten komplexen Krankheitsprobleme wird so auf viele Expertenschultern verteilt, um den für den Patienten höchsten Effizienzgrad mit dem Ziel des optimalen Behandlungserfolges zu erreichen. Diese intensive Art der Behandlung übersteigt die Leistungen der „Regelversorgung“ und wird – wenn überhaupt – aus den Mitteln des Forschungsverbundes finanziert. Insbesondere ist sie in Abgrenzung zur reinen Behandlungsdokumentation oder gewöhnlichen Patientenakte mit einem deutlich erhöhten Dokumentationsaufwand verbunden. Ob dieser erhöhte Dokumentations- und Kommunikationsaufwand tatsächlich mit einem verbesserten Behandlungserfolg einhergeht, ist im Idealfall Gegenstand einer systematischen Versorgungsforschung.

Für diese und weitere ähnliche Szenarien stellt das Klinische Modul einen Mechanismus bereit, der die Erhebung und Verarbeitung von klinischen Forschungsdaten weitgehend in den Behandlungsprozess integriert. Wesentliche Merkmale dieser Integration sind:

- Erstbehandler stellen den Kontakt zwischen dem Patienten und dem Forschungsverbund her. Dazu gehören Aufklärung und Einholung der Einwilligungserklärung hinsichtlich der Teilnahme des Patienten an dem Forschungsverbund, sowie die Erfassung des Patienten im Klinischen Modul.
- Erstbehandler und weitere Behandler haben Onlinezugriff auf identifizierende Daten (IDAT) und medizinische Daten (MDAT), solange ein Behandlungsverhältnis zum jeweiligen Patienten besteht.
- Alle Behandler dokumentieren ihre jeweiligen Erkenntnisse in einem gemeinsamen medizinischen Datenbestand (MDAT), der in einer zentralen Klinischen Datenbank gespeichert wird.

- Alle Behandler können im Umgang mit der Online-Datenerfassung des Klinischen Moduls die im jeweiligen Behandlungszusammenhang üblichen identifizierenden Patientendaten (Name, Vorname, Versichertennummer, usw.) nutzen.

Der Kern des Klinischen Moduls besteht aus einer Klinischen Datenbank (KDB), die ausschließlich medizinische Daten (MDAT), jedoch keine Identitätsdaten (IDAT) enthält; je nach organisatorischen Anforderungen (z.B. Trennung nach Krankheits-Subentitäten) kann das Klinische Modul auch mehrere Klinische Datenbanken beherbergen. Die Identitätsdaten werden in einer getrennten Patientenliste (PL) gehalten. Beide Datenbestände sind über einen gemeinsamen Schlüssel PID_K verknüpft, der ausschließlich zwischen diesen beiden Systemen kommuniziert wird, ansonsten jedoch geheim bleibt. Die beiden Komponenten Klinische Datenbank und Patientenliste müssen räumlich getrennt angeordnet sein und dürfen nicht derselben Daten verarbeitenden Stelle unterstehen. In einer Klinischen Datenbank wird also das Prinzip einer pseudonymen Speicherung bei gleichzeitig personenbezogenem Zugriff im Behandlungszusammenhang umgesetzt.

Innerhalb des Behandlungsgeschehens haben Berechtigte Zugriff auf die Klinische Datenbank und die Patientenliste und können – wie in den meisten Behandlungsszenarien üblich – mit dem Patienten namentlich kommunizieren. Im Forschungsumfeld besteht kein Zugriff auf die Patientenliste, so dass hier nur pseudonymisierte medizinische Daten zur Verfügung stehen. Ein Rückgriff auf die Identitäten ist nur unter Mitwirkung des Betreibers der Patientenliste möglich, so dass diesem treuhänderische Aufgaben zufallen.

Im Gegensatz zu einem Studienmodul (s. Kap. 5.2) steht im Klinischen Modul die Behandlung der Patienten im Vordergrund, wird aber z.B. im Sinne einer Beobachtungsstudie wissenschaftlich begleitet und ausgewertet. Das Forschungsziel ist im Gegensatz zum Studienmodul nicht von vornherein durch Hypothesen eng umrissen, entsprechend kann die nötige Aufbewahrungsdauer der Daten unbestimmt sein. Diese Offenheit bringt erhöhte Anforderungen an Patientenaufklärung und -einwilligung mit sich und erfordert ein im Vergleich zum Studienmodul strengeres Pseudonymisierungsverfahren – das verwendete Pseudonym ist im Gegensatz zum SIC des Studienmoduls (s. Kap. 5.2) dem behandelnden Arzt nicht bekannt.

Auch versorgungsnahe Register, z.B. klinische Krebsregister oder klinische Datawarehouses, können bei entsprechender Konstruktion durch ein Klinisches Modul modelliert werden. Das gleiche gilt für wissenschaftsgetriebene Studien (IIT), soweit sie nicht unter die Regularien von AMG und MPG fallen.

Typisch für Verbünde, die nur ein Klinisches Modul haben, ist die auf einen langen Zeitraum ausgerichtete Datensammlung, die besondere datenschutzrechtliche Überlegungen und Maßnahmen erfordert. Wichtig ist hier, dass der Verbund oder die zentrale Datenbank selbst „die Studie" ist, auf die sich

die Einwilligung bezieht, sodass nicht für jedes Teilprojekt, das die Daten verwendet, neue Einwilligungen eingeholt werden müssen. Natürlich bewirkt eine umfassende, sogar über eine elektronische Patientenakte hinausgehende Dokumentation mit erweiterter Datenerfassung für aktuelle oder künftige Forschungsfragen einen erhöhten Schutzanspruch, der zwingend zusätzliche Schutzmaßnahmen nach sich zieht. In einem größeren Netz werden die Daten des Klinischen Moduls (im nötigen Umfang) für Forschungszwecke in der Regel in andere Module übertragen. Die Konstruktion des Klinischen Moduls erlaubt aber auch, insbesondere für kleinere Netze, Forschungsfragen direkt mit den Daten des Klinischen Moduls anzugehen. Dafür ist ein anonymisierter oder, falls dieser nicht zielführend ist, ein pseudonymisierter Export vorgesehen. Für einfache Auswertungen, auch ökonomischer Fragestellungen, reicht dabei in der Regel ein anonymisierter Export.

Das Klinische Modul kann durch eine Bilddatenbank oder eine Biobank ergänzt werden. Hierbei sind zwei Varianten denkbar, die sich durch den Anknüpfungspunkt der zusätzlichen Datenbanken unterscheiden:

- Die Bilddatenbank bzw. Biobank kann über ein eigenes Pseudonym mit der Patientenliste verknüpft werden. Die Zusammenführung – auch zu Forschungszwecken – erfordert dann immer einen Rückgriff auf die Patientenliste, auch wenn die IDAT hierfür nicht benötigt werden. Dafür wird das Reidentifizierungsrisiko der Klinischen Datenbank nicht erhöht.
- Alternativ können Bilddatenbank und Biobank ohne direkte Anbindung an die Patientenliste geführt und dafür über geeignete Schlüssel mit der Klinischen Datenbank verbunden werden. Dadurch wird der Datensatz der Klinischen Datenbank effektiv verbreitert.

Eine genauere Beschreibung dieser Anbindung ist im Kapitel 6.5 zum Maximalmodell bzw. Kapitel 5.4 zum Biobankenmodul und dem ausführlicheren generischen Datenschutzkonzept für Biomaterialbanken [2] zu finden.

In einer Klinischen Datenbank können auch Daten von Sensoren am Patienten und unterstützenden technischen Geräten („AAL-Daten“) gespeichert werden; solche Daten sind den medizinischen Daten zuzuordnen. Die datenschutzgerechte Gewinnung und Übermittlung solcher Daten sowie ihre Qualitätssicherung bedürfen gesonderter Überlegungen, die nicht Gegenstand dieses generischen Datenschutzkonzepts für medizinische Forschungsverbünde sein können. Werden in diesem Kontext Daten vom Patienten selbst eingegeben, so entspricht dies der in Kapitel 5.2.4 beschriebenen Situation.

5.1.2 Anwendungsfälle

5.1.2.1 Patienten in das Klinische Modul aufnehmen

Als Erstkontakt aus Sicht des Forschungsverbunds ist derjenige Kontakt mit dem Erstbehandler zu werten, der – nach entsprechender Aufklärung und Ein-

holung der Einwilligung (vgl. Kap. 3.2.3.1) – zu einer Aufnahme des Patienten in den Forschungsverbund führt. Hier wird im Wesentlichen ein Eintrag in der Patientenliste erzeugt und ein Basisdatensatz in der Klinischen Datenbank hinterlegt. Ist der Patient bereits mit gleichen oder ähnlichen Angaben in der Patientenliste eingetragen, so ordnet das System den Patienten nach Möglichkeit richtig zu und weist, wenn das nicht zweifelsfrei möglich ist, auf die mögliche Verwechslungsgefahr hin. Es ist darauf zu achten, dass dabei nicht die Identität eines anderen Patienten enthüllt wird.

5.1.2.2 Rechte an Mit- und Weiterbehandler vergeben

Die Autorisierung von Mitbehandlern hinsichtlich des lesenden Zugriffs auf die zentral gespeicherten Daten erfolgt grundsätzlich durch einen Vorbehandler in Absprache mit dem Patienten oder durch den Patienten selbst; die Umsetzung wird, soweit sie nicht automatisiert ablaufen kann, durch einen zuständigen Systemadministrator (Datenmanager, evtl. Rechtemanager) vorgenommen. So wird z.B. ein Hausarzt bei der Überweisung an eine Spezialklinik vorab die Überweisung selbst und die Erteilung der Zugriffsberechtigung mit dem Patienten besprechen und dann online erteilen, oder, je nach Organisation des Forschungsverbunds, dem Rechtemanagement einen entsprechenden Auftrag erteilen. Die Autorisierung kann explizit einem aktuellen Mit- oder Weiterbehandler erteilt werden. Optional kann sie auch für zukünftige Behandler erteilt werden. Diese Autorisierungen werden in der Patientenliste oder in einem separaten Rechtemanagement geeignet hinterlegt.

5.1.2.3 Daten im Behandlungsprozess erheben

Grundsätzlich kann jeder Behandler nur auf die von ihm bzw. von seiner Dienststelle selbst eingegebenen Daten lesend und schreibend (nachträgliche Änderungen werden protokolliert) zugreifen. Durch eine entsprechende Autorisierung (s. o.) kann einem Mit- oder Nachbehandler Einsicht in die Daten gewährt werden.

5.1.2.4 Behandlungsqualität sichern

Zugriffe zum Zweck der Qualitätssicherung können sich entweder an einzelnen, sachlich zusammenhängenden Angaben im gesamten Bestand oder an breit gefächerten Angaben zum einzelnen Patienten orientieren. Letzteres kann nur durch (Mit-)Behandler erfolgen. Der ausschließlich lesende Zugriff auf begrenzte MDAT kann einzelnen Qualitätsbeauftragten (s. Kap. 5.1.4.6) erteilt werden. Hier ist jedoch der Zugang zu den Identitätsdaten der Patientenliste verwehrt. Außerdem ist darauf zu achten, dass nicht durch die Häufung von Funktionen in der Qualitätssicherung in einer Hand eine Reidentifizierung möglich wird.

5.1.2.5 Expertenforum organisieren

In einigen medizinischen Forschungsverbünden ist die Einrichtung von Expertenforen sinnvoll, in denen ausgewählte Experten medizinische Aspekte von Erkrankungsfällen diskutieren. Dieses Szenario ist vor allem bei seltenen Erkrankungen von Bedeutung, aber auch in anderen Verbünden, wenn es um schwierige Diagnosen und Therapieempfehlungen geht. Die Experten können gezielt angefragt werden oder von sich aus Kommentare zu einem Fall abgeben. Dabei handelt es sich auch haftungsrechtlich nicht um ein Konsil, das auf einem Auftragsverhältnis im Behandlungszusammenhang beruht und in der Regel personenbezogen durchgeführt wird. Im Expertenforum werden Daten nur pseudonymisiert bereitgestellt.

a) Fragestellungen für ein Expertenforum: Aufgabe ist die fallbezogene Diskussion zu einer Erkrankung. Konkrete Fragen zu Diagnose oder Therapie können gestellt werden; es sollen aber auch spontane Beiträge möglich sein, die Hypothesen oder Ideen formulieren. Ergebnisse kommen dem behandelten Patienten direkt zugute.

b) Teilnehmerkreis: Teilnehmer des Forums sind namentlich benannte Experten, die persönlich zum Forum zugelassen werden. Diese können auch im Ausland ansässig sein. Die Liste der Experten sollte dem betroffenen Patienten, idealerweise sogar öffentlich bekannt sein. Empfohlen wird, eine solche Liste kontinuierlich aktualisiert im Web bereit zu stellen. Die Einbindung eines Expertenforums muss durch die Einwilligungserklärung der Patienten abgedeckt sein. Dort ist ggf. auch auf die Möglichkeit der Einbindung ausländischer Experten explizit hinzuweisen.

c) Datenspeicherung und Datenzugang: Die Daten werden in der Klinischen Datenbank gespeichert. Der Online-Zugang für die Experten ist für die Dauer der Diskussion befristet, etwa 2 bis 4 Wochen; danach wird der Zugang zum jeweiligen Fall wieder gesperrt.

d) Personenbezug: Der Bezug auf die Identitätsdaten ist in diesem Szenario nicht notwendig; andererseits ist eine Verständigung nötig, auf welchen Fall sich die Diskussion bezieht. Daher ist die Einführung eines Pseudonyms speziell für diesen Zweck nötig. Der jeweils im persönlichen Behandlungszusammenhang stehende Arzt, ggf. auch Konsiliar, muss das Pseudonym dem konkreten Patienten zuordnen können. Nach Ablauf der Diskussionsfrist wird der Zugang zu den Falldaten und zum Pseudonym außer für behandelnde Ärzte gesperrt. Das Pseudonym muss allerdings in der Datenbank verbleiben, um auch später eingehende Beiträge zu diesem Fall noch zuordnen zu können und auch, um die Dokumentation der vorher eingegangenen Beiträge nachvollziehbar zu halten.

5.1.2.6 Datenqualität sichern

Für die Datenqualitätssicherung sind unter Umständen umfangreiche Datenzugriffe notwendig (s. dazu Kap. 6.8). Auch Monitoring-Prozesse können im Klinischen Modul vorgesehen sein.

5.1.2.7 Auskunft geben

Die Patienten haben ein Recht auf Auskunft über die von ihnen gespeicherten personenbezogenen Daten. Zudem sind diese auf Verlangen der Patienten auch zu korrigieren (vgl. Kap. 4.4.1). Der Patient wendet sich hierzu an den aktuell behandelnden Arzt, der Zugriff auf den vollständigen Datensatz des Patienten hat und diesem entsprechend Auskunft geben kann. Vom Patienten gewünschte Änderungen sind, sofern medizinisch unproblematisch, vom behandelnden Arzt vorzunehmen. Sollten Änderungen gewünscht werden, die einer medizinisch korrekten Dokumentation widersprechen, muss dies ggf. als Rückzug der Einwilligung gewertet werden, so dass der betreffende Datensatz zu löschen oder zu anonymisieren ist. Der behandelnde Arzt muss verhindern, dass durch Korrekturen oder Löschungen ein aus medizinischer Sicht unzutreffendes Bild des Patienten und der Behandlung gezeichnet wird.

5.1.2.8 Daten sperren, anonymisieren oder löschen

Die Löschung oder Sperrung kann vom Patienten über jeden teilnehmenden Behandler oder über die Netzwerkzentrale beantragt werden. Sie führt ggf. zur Entfernung des Eintrags aus der Patientenliste sowie zur Sperrung aller klinischen Daten (MDAT). Optional kann der Patient einer Anonymisierung zustimmen. Die Durchführung obliegt in jedem Fall dem Betreiber der jeweiligen Datenbank.

Generell sollte bereits mit der Aufnahme eine Vereinbarung über den Verbleib der gesammelten Daten im Todesfall getroffen werden. Im Klinischen Modul ist im Todesfall mindestens die Löschung oder Sperrung der IDAT in der Patientenliste erforderlich.

5.1.2.9 Machbarkeit einer Auswertung oder Studie prüfen

Die Fallsuche dient im Wesentlichen der Feststellung, ob eine gegebene Fragestellung mit dem aktuellen Bestand mit Aussicht auf Erfolg bearbeitet werden kann. Sie kann von entsprechend autorisierten Wissenschaftlern online vorgenommen werden. Bei der Fallsuche werden nur aggregierte Daten (Fallzahlen, Mittelwerte, etc.) bereitgestellt und für die Ausgabe der Ergebnisse von Datenbankabfragen Mindestanzahlen von Datensätzen festgelegt; dadurch soll verhindert werden, dass durch geschickt formulierte Abfragen einzelne Datensätze identifiziert werden können. Der Zugriff auf Identitätsdaten

bleibt verwehrt, ebenso der Zugriff auf einzelne MDAT-Sätze. Dieses Verfahren ist auch im Forschungsmodul enthalten, siehe Kapitel 5.3.2.4, und kann ggf. auch zur Schätzung von Inzidenzen verwendet werden.

5.1.2.10 Rekrutierung unterstützen

Um Patienten für klinische Studien zu rekrutieren, ist letztlich ein Rückgriff auf MDAT und IDAT notwendig. Das Klinische Modul kann ein besonders effizientes Verfahren bereitstellen. Dabei werden gezielt die behandelnden Ärzte informiert, deren gemeldete Patienten für eine spezifizierte Studie geeignet sind. Diese sind letztlich für die eigentliche Rekrutierung verantwortlich. Alternativ können für eine Rekrutierung durch Dritte mittels konsekutiven Zugriffs auf Klinische Datenbank und Patientenliste geeignete Listen erstellt und daraufhin die Patienten kontaktiert werden, sofern eine entsprechende Einwilligung vorliegt.

5.1.2.11 Daten an Forscher weitergeben

Der Export medizinischer Daten zu Forschungszwecken erfolgt nach wissenschaftlicher, ethischer und datenschutzbezogener Begutachtung durch entsprechende Gremien. Verantwortlich für den eigentlichen Export (nach Auftrag durch die entsprechenden Gremien) ist der Betreiber der Klinischen Datenbank. Der Export erfolgt wenn möglich anonymisiert, sonst pseudonymisiert. Ein Onlinezugriff ist nicht vorgesehen.

5.1.2.12 Ergebnisse mitteilen

Im Rahmen wissenschaftlicher Auswertungen pseudonym exportierter Daten des Klinischen Moduls können Ergebnisse entstehen, die für die weitere Behandlung einzelner Patienten relevant oder zumindest von Interesse sein können. In so einem Falle wird zunächst geprüft, ob die Rückmeldung solcher Ergebnisse mit dem Patienten vereinbart wurde, oder ob eine dringende medizinische Notwendigkeit besteht, die Ergebnisse mitzuteilen. Wenn eine Mitteilung erforderlich oder gewünscht ist, wird im Regelfall der aktuell behandelnde Arzt informiert und über das Ergebnis der Auswertung in Kenntnis gesetzt. Dieser informiert dann den Patienten über das Ergebnis und berät ihn hinsichtlich möglicher Konsequenzen. In Ausnahmefällen und falls in dieser Form mit dem Patienten vereinbart, kann auch eine Kontaktierung direkt durch den Forschungsverbund stattfinden.

5.1.3 Daten und Datenflüsse

Der Datenbestand des Klinischen Moduls entsteht durch die kontinuierliche interaktive Nutzung des Moduls im Behandlungszusammenhang. Darüber

hinaus sind Übermittlungen größerer Datensätze in oder aus der Klinischen Datenbank im Rahmen des Klinischen Moduls kaum erforderlich.

Der Zugriff auf MDAT identifiziert durch IDAT während der Erst-, Weiter- oder Mitbehandlung erfolgt in drei Schritten. Nach Prüfen der Berechtigung und nach Auffinden des Patienten in der Patientenliste wird ein weiteres, nur für diesen konkreten Vorgang verwendetes temporäres Pseudonym – hier Zugriffsticket (TKT) genannt, im Modell A des bisherigen generischen Datenschutzkonzepts als TempID bezeichnet – erzeugt und an den Berechtigten sowie an die Klinische Datenbank übermittelt. Der Berechtigte erhält mit dem TKT Zugriff auf die entsprechenden MDAT. Dabei ist die Gültigkeitsdauer des TKT auf den Zeitbedarf einer typischen Arbeitssitzung beschränkt. Der technische Ablauf wird in der Abbildung 14 im Kapitel 6.1 zum Identitätsmanagement beschrieben.

Die Erzeugung eines TKT kann unterbleiben, wenn für einen bestimmten Vorgang nur der Zugriff auf eine der beiden Komponenten erforderlich ist. Beispiele hierfür sind ein Update der IDAT, z.B. nach Namensänderung, oder ein Export von Forschungsdaten.

Das im Klinischen Modul verwendete Pseudonym PID_K wird zu keinem Zeitpunkt an einem weiteren Ort außer der Patientenliste und den Klinischen Datenbanken, in denen der Patient geführt wird, gespeichert.

Datenflüsse zwischen dem Klinischen Modul und evtl. vorhandenen weiteren Modulen des Forschungsverbundes werden in Kapitel 6 beschrieben, insbesondere in den Kapiteln 6.3 und 6.5. Der direkte Datenexport aus der Klinischen Datenbank zu Forschungszwecken ähnelt dem aus der Forschungsdatenbank, sofern dort kein Online-Zugriff vorgesehen ist, siehe Kapitel 5.3.2.9.

Externe Forscher können, da für den Export stets neue (Einmal-)Pseudonyme verwendet werden, selbst kein Follow-up durchführen, sondern benötigen im Bedarfsfall immer einen Export der gesamten Historie. Dadurch wird insbesondere der Aufbau einer externen Schatten-Datenbank verhindert.

5.1.4 Nutzer, Rollen und Rechte

Das Klinische Modul betrachtet überwiegend die Rollen des behandelnden Arztes (in der Regel mehrere Ärzte für jeden einzelnen Patienten) und des Wissenschaftlers, dazu verschiedene Systemadministratoren.

5.1.4.1 Behandelnder Arzt

Die im Behandlungsprozess tätigen Ärzte erwarten von einer klinisch fokussierten Vernetzung eine Optimierung ihrer Prozessstrukturen, um so Diagnostik und Therapie für ihre Patienten verbessern zu können. Da die suffiziente Zuarbeit der Kliniker zur Forschung auch bei maximaler technischer Hilfe-

stellung, nicht zuletzt durch den zusätzlichen Aufwand bei der Patientenführung und -aufklärung, immer Mehrarbeit erfordert, erwarten die klinisch tätigen Ärzte von der klinisch-wissenschaftlichen Vernetzung des Klinischen Moduls darüber hinaus eine Verminderung redundanter Arbeitsvorgänge. Daraus ergeben sich die nachfolgenden Anforderungen:

- Der Zugriff auf krankheitsbezogene Informationen der Patienten muss verwechslungsfrei und fehlerlos möglich sein. Die Erfassung jeglicher patientenbezogener Daten muss der Fortschreibung einer Krankengeschichte dienen und bei einer Wiedervorstellung des Patienten verfügbar sein, auch – mit Einwilligung des Patienten – bei einem Wechsel des Behandlers.
- Die im Forschungsdatensatz definierten Informationen aus allen im Forschungsnetz teilnehmenden diagnostischen und therapeutischen Bereichen (z.B. Arztpraxis, Klinik, Labor), die im Behandlungsprozess erforderlich sind, sollen patientenbezogen zeitnah und lückenlos zusammengeführt werden können, um so den Informationsstand zwischen den am Behandlungsprozess Beteiligten zu optimieren.
- Die Doppelerfassung klinischer Daten zur wissenschaftlichen Dokumentation muss, soweit möglich, vermieden werden, die Ableitung der wissenschaftlich relevanten Daten aus den klinischen Daten ist aus Gründen der Arbeitserleichterung und der Qualitätssicherung anzustreben.
- Die Suche nach eigenen Patienten anhand beliebiger Suchkriterien sowie einfache Auswertungen über eigene Patienten sollten möglich sein.

Führen wissenschaftliche Untersuchungen zu Ergebnissen, die für den individuellen Patienten relevant sind, so muss der behandelnde Arzt in die Lage versetzt werden können, mit diesem Patienten Kontakt aufzunehmen, um den Behandlungsprozess an die neue Situation anzupassen.

5.1.4.2 Laborarzt

Auch Laborärzte können als behandelnde Ärzte registriert werden, sofern diese einen Untersuchungsauftrag erhalten, der ein für die Behandlung des Patienten relevantes Ergebnis ergibt. Laborärzte erhalten einen eingeschränkten Zugang zu den klinischen Daten des Patienten in Abhängigkeit von der durch sie zu erbringenden Untersuchung. Sie können ihr Ergebnis – sofern dieses im Datensatz des Forschungsnetzes vorgesehen ist – online in den klinischen Datenbestand eingeben. Laborärzte werden von den behandelnden Ärzten direkt beauftragt und erhalten dadurch Zugang zur Klinischen Datenbank.

5.1.4.3 Wissenschaftler

„Wissenschaftler“ oder „Forscher“ kommen in einem Forschungsverbund in verschiedenen Varianten vor und müssen in ihrer Rolle dementsprechend differenziert werden:

- der Leiter des Forschungsverbunds oder eines zentralen Teilprojekts (Studienleiter) und seine Mitarbeiter, die mit den anfallenden Daten neue Erkenntnisse gewinnen wollen,
- teilnehmende Ärzte mit eigenen Forschungsinteressen,
- das „biostatistische Personal" des Forschungsverbunds, das die Auswertungen direkt vornimmt,
- externe Forscher, die Daten (evtl. auch Proben) zur Erforschung eigener Fragestellungen übermittelt bekommen, z.B. Epidemiologen oder Vertreter der Industrie; dieser Gruppe ist auch ein medizinischer Qualitätsbeauftragter, siehe Kapitel 5.1.4.6, zuzuordnen,
- Experten als Teilnehmer an einem Expertenforum, die durch die Diskussion seltener Fälle Ideen und Hypothesen für neue Forschungsansätze gewinnen können.

Die beteiligten leitenden Wissenschaftler erwarten durch die Teilnahme am Forschungsnetz nicht nur, mehr Patienten in ihre Forschung einzubringen, sondern auch den klinischen Bezug ihrer Forschung besser herstellen zu können. Gerade bei chronischen und besonders schweren oder seltenen Erkrankungen sind Rückgriffe auf fallbezogene frühere Informationen und frühere biologische Proben oftmals von besonders großem Interesse, wenn Prognose und Therapieeffekte betrachtet werden sollen. Die Anforderungen der Wissenschaftler betreffen daher besonders folgende Punkte:

- Die zentrumsübergreifende Zusammenführung von diagnostischen und therapeutischen Daten soll helfen, eine möglichst große Zahl Patienten der wissenschaftlichen Evaluation zur Verfügung zu stellen.
- Eine übergreifende epidemiologische Aus- und Bewertung der fallbezogenen Informationen muss möglich sein.
- Der Zusammenhang der klinisch erhobenen Daten mit den Ergebnissen der Forschung, z.B. an biologischen Proben, muss hergestellt werden können, um so die Wertigkeit der Untersuchung für den Behandlungsfall besser beurteilen zu können.

Sonstige teilnehmende Ärzte ohne eigentliche Forschungsinteressen sollen Auswertungen über ihre eigenen Patienten machen können oder im Sinne des Benchmarking vergleichende Statistiken anfordern können; deren Anfertigung fällt in den Aufgabenbereich des Qualitätsbeauftragten.

5.1.4.4 Administrator für die Patientenliste (PL)

Der Betrieb einer Patientenliste wird in Kapitel 6.1 zum Identitätsmanagement näher erklärt. Im Zusammenhang mit dem Klinischen Modul ist festzuhalten, dass zusätzlich zu den Identitäten auch die Behandlungsbeziehungen zwischen Ärzten und Patienten in geeigneter Weise ermittelt und abgebildet werden müssen. Dem Administrator der Patientenliste obliegt im Wesentlichen die Überwachung der Zugriffe im Behandlungszusammenhang. Zu den Auf-

gaben des Administrators gehören auch manuelle Korrekturen bei Falscheingaben in die Patientenliste oder bei softwareseitig unauflösbaren Namenskonflikten.

5.1.4.5 Administrator für eine Klinische Datenbank (KDB)

Der Betrieb einer Klinischen Datenbank erfolgt weitgehend unabhängig von der Patientenliste. Jedoch müssen beide Datenbanken kompatible Identitätsmerkmale verwenden. Dazu gehört sinnvollerweise, wenn auch nicht zwingend erforderlich, die Verwendung der gleichen Benutzernamen, z.B. im Rahmen eines netzweiten einheitlichen Benutzer- und Rechtemanagements.

5.1.4.6 Qualitätsbeauftragter

Der Qualitätsbeauftragte bearbeitet Fragestellungen der medizinischen Qualitätssicherung und des Benchmarkings. Das erfordert das Aufstellen vergleichender Statistiken. Hierzu benötigt er Zugriff auf geeignete exportierte Teildatensätze der MDAT. In seiner technischen Rolle und seinen Rechten unterscheidet er sich nicht von einem externen Forscher.

5.1.4.7 Klinischer Monitor

Im Klinischen Modul kann auch ein Monitoring-Verfahren vorgesehen sein; im Gegensatz zum Studienmodul ist dieses hier aber optional. Das Verfahren unterscheidet sich jedoch nicht von dem in Kapitel 5.2.4 beschriebenen.

5.1.5 Verantwortlichkeiten

Allgemeine Aussagen, die für alle Forschungsverbünde gelten, sind in Kapitel 6.6, Organisatorische Regelungen, zusammengefasst.

Zentrales Merkmal des Klinischen Moduls ist die Trennung von identifizierenden und medizinischen Daten in Patientenliste und Klinischer Datenbank, die durch verschiedene Daten verarbeitende Stellen betrieben werden. Damit soll unterbunden werden, dass eine Stelle Kontrolle über beide Datenbestände erhält. Beide Betreiber sind verpflichtet, unabhängige Zugangsmechanismen und Zugangsprotokolle vorzuhalten, müssen aber einheitliche Zugriffsrichtlinien implementieren, wobei ein zentrales Rechtemanagement hilfreich sein kann. Dieses kann auch in die (Standard-)Benutzerverwaltung der Klinischen Datenbank integriert sein, sofern deren Administration dadurch nicht zu Interessenskonflikten führt.

Ferner muss die Nutzung der MDAT zu Forschungszwecken bzw. der IDAT zu Zwecken der Benachrichtigung bei besonderen Erkenntnissen oder der Rekrutierung für Studien durch den Ausschuss Datenschutz kontrolliert werden.

Dieser weist den jeweiligen Administrator der Klinischen Datenbank bzw. der Patientenliste entsprechend an.

5.1.6 Besondere Aspekte der Realisierung

Software, die für das Datenmanagement des Klinischen Moduls geeignet ist, fällt in eine von drei Kategorien:

- web-basierte Lösungen, die mit Hilfe eines Webservers, einer dahinter liegenden Datenbank und interaktiven Webseiten „selbst gestrickt" werden,
- EDC-Systeme,
- EPA-Systeme (wenn eine pseudonyme Datenhaltung unterstützt wird).

Es gibt aber bisher keine auf dem Markt verfügbare Software, die die Anforderungen an ein Klinisches Modul in einem Forschungsverbund vollständig abdeckt. Schwachpunkt ist die Erfüllung der Notwendigkeit, MDAT und IDAT nirgends außer auf dem Client-Rechner eines behandelnden Arztes gleichzeitig erscheinen zu lassen. Bei einem web-basierten System, bei dem Standard-Browser als Clients verwendet werden, besteht zwar grundsätzlich die Möglichkeit, aus einem einzigen Webformular Daten von verschiedenen Servern abzurufen. Diese als „Cross-Site-Scripting" bekannte Möglichkeit wurde in der Vergangenheit aber als schwerwiegende Sicherheitslücke diskreditiert und wird daher in gängigen Sicherheitseinstellungen unterbunden. Derzeit können drei mögliche Realisierungsvarianten unterschieden werden:

1. Bei einer Auftrags- oder Eigenprogrammierung können solche technischen Möglichkeiten der Datenzusammenführung im Webbrowser genutzt werden[20], die derzeit nicht als Cross-Site-Scripting angesehen und unterdrückt werden. Für einfach gestaltete Szenarien lassen sich so vergleichsweise leicht umzusetzende Software-Lösungen zur Verfügung stellen.
2. Für gehobene Ansprüche – von denen man zumindest in größeren Forschungsverbünden ausgehen muss – wird man in der Regel anstreben, ein kommerzielles Datenmanagementsystem (EDC- oder RDE-System) einzusetzen, wie es vor allem für klinische Studien auf dem Markt angeboten wird. Solche Systeme halten die strikte Trennung zwischen IDAT und MDAT bisher in der Regel aber nicht ein. Verwenden sie für die Applikationslogik einen von der Datenbank getrennten Anwendungsserver, so lässt sich die Datenzusammenführung auf diesen beschränken. Im besonders zu prüfenden Einzelfall könnten die Anforderungen des Klinischen Moduls dann insofern erfüllt werden, als der Anwendungsserver von einem unabhängigen Datentreuhänder betrieben wird.

20 Z.B. auch ein von der Universität Münster zusammen mit der TMF angebotenes Werkzeug, siehe http://www.tmf-ev.de/Produkte/P014012

3. Eine dritte Umsetzungsvariante besteht in dem Einsatz einer entsprechenden Proxy-Software in jeder behandelnden Einrichtung, die die getrennte Anforderung von IDAT und MDAT und die zusammengeführte Weiterleitung an den Client übernimmt[21].

Näher an den Bedürfnissen der klinischen Dokumentation sind vermutlich bestehende Softwaresysteme zur Abbildung von elektronischen Patienten- oder Krankenakten (EPA). Bei diesen Systemen ist die pseudonyme Speicherung samt getrennter Datenhaltung von MDAT und IDAT ebenfalls eine kritische Anforderung. Auch für solche Softwaresysteme ist zu klären, welche der möglichen Varianten einer abgesicherten Zusammenführung von IDAT und MDAT umgesetzt wird.

Die ohnehin strikt empfohlene kryptographische Absicherung aller Datenübertragungswege hilft im Klinischen Modul auch, die Trennung von MDAT und IDAT besonders effektiv umzusetzen: Wenn beide Übertragungswege, d.h. von der Klinischen Datenbank und von der Patientenliste zum peripheren Client, vollständig verschlüsselt sind und sich die Datenströme nicht außerhalb des Clients treffen, kann ein unbefugter Reidentifikationsversuch auch nicht mit Hilfe eines Abhörens des Netzes unternommen werden.

Das Thema der Selbstdokumentation durch Patienten stellt sich im Klinischen Modul genau so wie im Studienmodul dar und wird dort behandelt, siehe Kapitel 5.2.4.

5.2 Studienmodul

5.2.1 Zweck und Anwendungsbereich

Das Studienmodul dient der sicheren Durchführung und Administration einzelner und klar voneinander abgegrenzter, klinischer Forschungsprojekte. Im Unterschied zum Anwendungsbereich des Klinischen Moduls steht jeweils eine explizit formulierte klinische Forschungsfrage im Vordergrund. Entsprechend konkret können Zweck und Dauer der Datenspeicherung angegeben werden, was ein im Vergleich zum Klinischen Modul vereinfachtes Pseudonymisierungsverfahren ermöglicht. Beispielhaft hierfür stehen klinische Studien zur Bewertung neuer oder neu eingesetzter Medikamente oder Medizinprodukte, die gemäß den gesetzlichen Bestimmungen des AMG oder MPG durchzuführen sind. Allerdings ist das Studienmodul in seiner Nutzbarkeit nicht auf solche gesetzlich geregelten Studien beschränkt.

21 Gerade in kleineren behandelnden Einrichtungen wie beispielsweise Arztpraxen könnte eine solche Zwischenstation zwischen dem öffentlichen Netz und dem Rechner des behandelnden Arztes auch aus Sicherheitsgründen befürwortet werden, weitere Hinweise in [weitere Hinweise in 30]

Das Studienmodul muss für einen forschenden Personenkreis, der ggf. keinen Behandlungsauftrag des Patienten und möglicherweise auch keinen direkten Kontakt zu dem Patienten hat, einen pseudonymisierten oder anonymisierten Zugriff auf die Patientendaten erlauben. Allerdings ist in den allermeisten Studien oft schon aus Sicherheitsgründen auch ein Rückschluss auf die Identität eines Patienten unter bestimmten Umständen notwendig, so dass sich die Verwendung anonymer Kennungen verbietet. Im Arzneimittelrecht ist zudem die Verwendung von Pseudonymen vorgeschrieben. Im Folgenden wird daher nur noch auf die pseudonymisierte Datenhaltung im Studienmodul eingegangen. Die pseudonymisierte Speicherung und Verarbeitung der Daten im Studienmodul setzt als Rechtsgrundlage in aller Regel eine informierte Einwilligung der Probanden voraus (vgl. Kap. 4). Prinzipiell ließe sich ein stark vereinfachtes Studienmodul auch mit anonymen Kennungen nutzen; einige Anwendungsfälle könnten dann jedoch nicht in der hier beschriebenen Form umgesetzt werden.

Für das Studienmodul wird keine doppelte Pseudonymisierung gemäß Modell B in der ersten Version der generischen Datenschutzkonzepte der TMF vorausgesetzt. Zusätzliche Schutzmaßnahmen werden erst erforderlich, wenn die Daten einer Studie oder eines Forschungsprojekts nach dessen Ende weiterhin in pseudonymisierter Form gespeichert und mit den Daten aus anderen Forschungsprojekten zusammengeführt werden sollen.

5.2.2 Anwendungsfälle

5.2.2.1 Patienten aufklären und Einwilligung einholen

Wenn die Kriterien und Voraussetzungen für die Aufnahme eines Patienten in eine klinische Studie gegeben sind, klärt der behandelnde Arzt oder Prüfarzt den Patienten umfassend auf und dokumentiert dessen schriftliche Einwilligung (vgl. Kap. 3.2.3.1). Dies kann nur an einer Stelle geschehen, wo die Aufbewahrung der identifizierenden Daten der Probanden unproblematisch ist. Im Regelfall ist dies die jeweilige ärztlich geleitete, behandelnde Einrichtung oder, im Falle einer übergreifenden Dateninfrastruktur, zusätzlich ein zentraler Datentreuhänder.

Als datenschutzrechtliche Besonderheit in klinischen Studien nach Arzneimittelrecht ist zu beachten, dass der Patient darüber aufzuklären ist, dass seine Daten auch nach einem Widerruf weiterhin verwendet werden, falls dies gemäß § 40 (2a) Satz 2 Nr. 3 AMG erforderlich ist, um Wirkungen des zu prüfenden Arzneimittels festzustellen, um sicherzustellen, dass schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden, oder um der Pflicht zur Vorlage vollständiger Zulassungsunterlagen zu genügen.

5.2.2.2 Patienten in eine Studie aufnehmen

Im Anschluss an die Dokumentation der schriftlichen Einwilligung wird für einen Patienten ein Subject Identification Code (SIC) als pseudonyme ID erstellt. Der SIC dient im Laufe der Studie zur Identifikation eines Datensatzes, gerade auch für die Kommunikation zwischen verschiedenen an der Studie beteiligten Personen.

5.2.2.3 Daten erheben

Die Erhebung von Studiendaten wird im Regelfall in Kenntnis des konkreten Probanden, aber nur unter Verwendung des Pseudonyms durchgeführt. Aus der Perspektive eines generischen Datenschutzkonzepts ist es dabei unerheblich, ob zunächst auf Papier dokumentiert wird und diese Bögen (CRF) in der behandelnden Einrichtung oder in einer durch die Studienleitung mit der die Datenerfassung und -verarbeitung beauftragten Studienzentrale in eine elektronische Studiensoftware (EDC) übertragen werden oder ob überhaupt keine Papier-Bögen mehr eingesetzt werden und direkt eine Eingabe in ein Studiensoftwaresystem erfolgt. Wichtig ist, dass in allen Fällen die Daten lediglich im Zusammenhang mit dem SIC als pseudonymer Kennung und ohne Einsicht in die identifizierenden Daten der Probanden dokumentiert werden.

Dabei können die Studiendaten eines Patienten ggf. auch in verschiedenen Einrichtungen oder durch verschiedene Studienärzte erhoben werden. In diesen Fällen ist zu klären, dass für alle beteiligten Stellen das Vorliegen der Einwilligung eindeutig dokumentiert ist und dass alle Daten mit dem gleichen SIC als pseudonymer Kennung für eine spätere Zusammenführung versehen werden.

5.2.2.4 Unerwartete Ereignisse managen

Unerwartete Ereignisse von medizinischer Relevanz können in jedem klinischen Forschungsprojekt auftreten und führen zu bestimmten Kommunikationsanforderungen. Besonders gesetzlich geregelt sind diese im AMG für klinische Studien mit einem besonderen, pharmakologisch begründeten Risikopotenzial für die Probanden. Neben der behandlungsseitigen, klinischen Dokumentation solcher Ereignisse ist somit auch eine Dokumentation im Zusammenhang mit dem Forschungsprojekt notwendig. Hierfür genügt im Regelfall die Zuordnung der medizinisch relevanten Daten zu dem Pseudonym des betroffenen Probanden.

In gesetzlich geregelten Studien nach AMG sind darüber hinaus auch gesetzliche Meldepflichten unerwünschter Ereignisse zu beachten. Die Kennzeichnung solcher Datensätze mit den Initialen und Geburtsdaten der Probanden, die in Anlehnung an internationale Empfehlungen [z.B. 31] bisher häufig verwendet wurde, ist nicht als ausreichende Pseudonymisierung anzusehen

[11, S. C34]. Die internationalen Vorgaben erlauben jedoch die Verwendung echter Pseudonyme in Kombination mit dem Alter des Probanden, wenn entsprechende nationale Vorgaben dies vorschreiben. Da im AMG die Pseudonymisierung der Daten in der Kommunikation mit dem Sponsor einer Studie vorgeschrieben ist und dieser wiederum für die Meldung unerwünschter Ereignisse gegenüber den Behörden verantwortlich ist, wird hierfür die durchgängige Verwendung der Pseudonyme – also hier der SICs – mit der Angabe des Alters und ohne Angabe des Geburtsdatums empfohlen. Dies gilt auch, wenn die Meldepflichten vom Sponsor an den Leiter der klinischen Prüfung oder andere Einrichtungen delegiert werden.

5.2.2.5 Datenqualität sichern

Auch die Prozesse der Qualitätssicherung klinischer Forschungsdaten sind mit einer Kommunikation pseudonymer Daten verbunden, wobei ein Kommunikationspartner die Zuordnung des Pseudonyms zum Patienten kennt und der andere im Regelfall nicht. So können im zentralen Datenmanagement Rückfragen zu den Daten eines Patienten formuliert werden, ohne dass die Identitätsdaten des Patienten hierfür benötigt werden. Wenn diese Rückfragen vom Studienarzt oder anderem ärztlich geführten Personal mit Patientenkontakt bearbeitet werden, geschieht dies im Regelfall in Kenntnis der Identität des betroffenen Patienten.

Ein wichtiges Verfahren zur Sicherstellung korrekter Daten in klinischen Studien ist das Monitoring. Dies wird durch speziell geschulte und hierfür beauftragte Personen durchgeführt, die in die beteiligten behandelnden Einrichtungen gehen und dort die erhobenen Daten mit den Quelldaten, im Regelfall den Patientenakten, abgleichen. Da dabei ein zusätzlicher Personenkreis Kenntnis personenbezogener Daten erhält, müssen die Patienten über dieses Verfahren aufgeklärt worden sein und dazu ihre Einwilligung gegeben haben (vgl. § 40 (2a) Satz 2 Nr. 1 Buchstabe a AMG).

Eine weitere Möglichkeit zur Sicherung einer hohen Datenqualität ist z.B. die Einbindung einer Referenzbefundung (vgl. Kap. 3.2.4.1).

5.2.2.6 Audit durchführen oder unterstützen

Durch Audits werden Prozessabläufe hinsichtlich der Erfüllung von Anforderungen und Richtlinien bewertet. Im Regelfall werden diese von speziell hierfür geschulten, unabhängigen und externen Fachleuten durchgeführt. Im Kontext von klinischen Studien ist ein Audit Bestandteil der Qualitätssicherung. Hierbei werden sämtliche Prozesse auf Übereinstimmung mit Studienplan, Richtlinien, SOPs und anderen verbindlichen Festlegungen – auch hinsichtlich Datenschutzmaßnahmen – geprüft. Ein Zugriff auf konkrete Daten ist, im Gegensatz zum Monitoring, allenfalls stichprobenartig nötig; ein Personenbezug muss im Regelfall nicht offenbart werden.

5.2.2.7 Auskunft geben

Die Patienten haben ein Recht auf Auskunft über die von ihnen gespeicherten personenbezogenen Daten. Zudem sind diese auf Verlangen der Patienten auch zu korrigieren (vgl. Kap. 4.4.1). Der Patient wendet sich hierzu an den zuständigen Prüf- bzw. Studienarzt, der Zugriff auf den vollständigen Datensatz des Patienten hat und diesem entsprechend Auskunft geben kann. Wenn im Falle einer AMG-Studie ein Patient die Entblindung seiner Studienmedikation verlangt, so ist dies nach Prüfung im Einzelfall entweder als Prüfplanverletzung umzusetzen und zu dokumentieren, oder auch als Rückzug der Einwilligung zu interpretieren, der einen Studienabbruch für diesen Patienten zur Folge hat.

5.2.2.8 Daten auswerten

Die Auswertung klinischer Forschungsdaten wird im Regelfall von Personen durchgeführt, die keinen direkten Patientenkontakt im Rahmen der Datenerhebung hatten und die die Identitätsdaten der Patienten nicht benötigen. In Einzelfällen kann es Abweichungen hiervon geben, wenn z.B. der Sponsor einer klinischen Prüfung mit dem Behandler identisch ist (s. Kap. 5.2.3.3 und 6.2.3.3). Somit können die Daten für die Auswertung in pseudonymisierter Form bereitgestellt werden, sofern hierfür Gründe vorliegen. Dies können z.B. Vorschriften aus dem AMG zur pseudonymisierten Weitergabe von Patientendaten an den Sponsor sein oder der Umstand, dass im Rahmen der Auswertung mit Ergebnissen zu rechnen ist, die möglicherweise eine personenbezogene Rückmeldung an einzelne beteiligte Probanden auch aus Patientensicht wünschenswert erscheinen lassen und eine solche Rückmeldung vereinbart wurde. Wenn kein Grund für die pseudonymisierte Auswertung vorliegt, werden die Daten in anonymisierter Form bereitgestellt.

5.2.2.9 Ergebnisse mitteilen

Nach Auswertung der Daten einer Studie werden den Patienten klinisch relevante Ergebnisse durch die behandelnden Ärzte mitgeteilt. Alternativ kann im Rahmen der Einwilligung vereinbart werden, weitere Ergebnisse mitzuteilen und auch den Kreis der mitteilungsberechtigten Personen zu erweitern.

5.2.2.10 Daten archivieren

Die Archivierung aller medizinisch relevanten Behandlungsunterlagen gehört zu den allgemeinen ärztlichen Dokumentations- und Aufbewahrungspflichten. Der hierfür relevante Rechtsrahmen ist auf eine Reihe allgemeiner (z.B. MBO, SGB-V) oder spezialgesetzlicher Regelungen (z.B. RöV, StrlSchV) verteilt. Im Rahmen klinischer Studien kommen Regelungen wie das AMG oder das MPG hinzu, die neben der ärztlichen Dokumentation eines Behandlungsfalls auch zusätzliche Daten und Dokumente fokussieren, die studienspezifisch sind.

Hierzu gehören z.B. die Einwilligungserklärungen der Probanden, die Dokumentation unerwünschter Ereignisse oder die Case Report Forms (CRFs) [9; 10].

Aus Datenschutzsicht relevant ist, dass auch bei der Archivierung der Studienunterlagen eine Aufteilung in Archive mit Identifikationsdaten und solche mit lediglich pseudonymisierten Daten möglich ist. Bei Studien nach AMG ist die Pseudonymisierung aller Unterlagen vorgeschrieben, die dem Sponsor übermittelt werden. Dieser hat entsprechend nur pseudonymisierte Daten zu archivieren, während der Prüfer z.B. auch die unterschriebenen Einwilligungserklärungen der Probanden rechtssicher aufbewahren muss [9].

5.2.2.11 Daten sperren, anonymisieren oder löschen

Die Probanden in klinischen Forschungsprojekten haben jederzeit das Recht, ihre Einwilligung in die Teilnahme zurückzuziehen. Im Regelfall sind dann alle zentral wie dezentral gespeicherten Daten zu löschen oder zu anonymisieren. Im Falle einer Anonymisierung sind die Identitätsdaten zu löschen, so dass zwischen diesen und einer vormals pseudonymen Kennung keine Beziehung mehr hergestellt werden kann. Wenn zusätzlich zu einer zentralen Patientenliste auch dezentrale Listen in den behandelnden Einrichtungen geführt werden, so sind auch in diesen die Einträge für den jeweiligen Probanden zu löschen. Wenn davon auszugehen ist, dass die pseudonyme Kennung aufgrund ihrer früheren Verwendung von einigen Personen nach wie vor dem konkreten Probanden zugeordnet werden kann, so sollte die vormalige pseudonyme Kennung durch eine neue anonyme ID ersetzt werden.

In klinischen Prüfungen gemäß Arzneimittelrecht ist zu beachten, dass auch bei einem Widerruf der Einwilligung bestimmte Daten nach § 40 (2a) Satz 2 Nr. 2 und 3 AMG weiterhin pseudonymisiert gespeichert werden müssen. Dies betrifft insbesondere die Notwendigkeit einer Übermittlung vollständiger Daten an die Oberbehörden im Rahmen eines Zulassungsverfahrens und Fälle, in denen die Sicherheit der Probanden anderenfalls nicht gewährleistet werden könnte. In Zweifelsfällen sollte zunächst zumindest eine Sperrung der Daten erfolgen.

Verstirbt ein Proband, so ist analog zum Rückzug der Einwilligung, inklusive der im AMG definierten Ausnahmeregelungen, zu verfahren. Eine anonymisierte Auswertung der bisher erhobenen Daten ist im Regelfall jedoch möglich.

5.2.2.12 Weitere Anwendungsfälle

Die folgenden Anwendungsfälle mit Behandlungsbezug sind prinzipiell auch im Studienmodul umsetzbar:

- Auskunft an weiterbehandelnden Arzt
- Zugriffsberechtigungsvergabe durch Vorbehandler oder Patient an weiterbehandelnden Arzt und Auskunft
- Zugriffsvergabe (Ausführung) durch Datenmanager oder Rechtemanager an weiterbehandelnden Arzt und Auskunft

Wie solche Anwendungsfälle konkret und vor allem IT-gestützt umgesetzt werden können, hängt jedoch sehr von der verwendeten Software, insbesondere für die Datenerfassung und das Studiendatenmanagement, ab. Kennzeichnend für das Studienmodul bleibt jedoch der Zugriff auf die zentrale Datenbasis mit Hilfe einer pseudonymen ID. Der Zugriff behandelnder Ärzte unter Verwendung der identifizierenden Daten der Patienten und die Regelungen zur dafür nötigen Zugriffsvergabe werden in dem Kapitel 5.1 zum Klinischen Modul sowie in den Kapiteln 6.1 und 6.2 zum Identitäts- und Rechtemanagement detailliert beschrieben.

5.2.3 Daten und Datenflüsse

5.2.3.1 Variante mit zentraler Patientenliste

Im Regelfall umfasst das Studienmodul drei Arten beteiligter Stellen:

1. die behandelnden Ärzte bzw. Prüfärzte, respektive die beteiligten Zentren,
2. eine zentrale Patientenliste samt Administration
3. und eine oder mehrere Studiendatenbanken mit dem zuständigen Personal.

Grundsätzlich können in einem Studienmodul mehrere Studien mit unterschiedlichen Studienzentralen parallel oder nacheinander durchgeführt werden, so dass ggf. eine große Zahl behandelnder Einrichtungen und auch mehrere Studiendatenbanken parallel zu verwalten sind. Es wird auch in solchen Konstellationen eine zentrale Patientenliste empfohlen.

Nach Einwilligung des Probanden in die Teilnahme am Forschungsprojekt wird das hierzu unterschriebene Dokument entweder in der behandelnden Einrichtung oder bei einer zentralen Stelle, die auch die Patientenliste verwaltet, aufbewahrt. Für den Probanden wird eine pseudonyme ID erzeugt, die an zentraler Stelle in der Patientenliste zusammen mit den identifizierenden Daten gespeichert wird. Der Studiendatenbank als zentralem Dokumentationssystem wird entweder eine projekt- oder studienübergreifende ID als PID_S oder ein studienspezifischer Subject Identification Code (SIC) zur Verfügung gestellt. Bei der Nutzung von SICs im Rahmen einer Studie ist eine spätere Zusammenführung von Daten möglich, wenn im zentralen ID-Management die unterschiedlichen SICs eines Patienten zusammen mit einem einheitlichen PID_S verwaltet werden. Die detaillierten Anforderungen an die Erzeugung solcher IDs sind im Kapitel 6.1 zum ID-Management beschrieben. Eine von der TMF zur Verfügung gestellte Software-Komponente hierfür, der PID-Generator, ist in Kapitel 6.1.6.1 dargestellt.

Die behandelnde Einrichtung erhebt die identifizierenden Daten (IDAT) der Probanden. Diese werden zusammen mit den Daten über die erhebende Stelle ($OrgDAT_{PL}$) verschlüsselt an die zentrale Patientenliste geschickt. Diese speichert IDAT und $OrgDAT_{PL}$ und schickt eine pseudonyme ID, entweder PID_S oder

SIC, an die behandelnde Stelle zurück. Die behandelnde Einrichtung dokumentiert alle weiteren Daten zum Probanden (MDAT) zusammen mit der pseudonymen ID (PID_S oder SIC) und schickt diese an die Studiendatenbank zur Speicherung der Daten zur Laufzeit der Studie.

Die Studiendatenbank und die Patientenliste stehen unter getrennter administrativer Aufsicht, es gibt keine übergreifende Weisungsbefugnis. Die jeweiligen Aufgaben und Befugnisse sind in den Regelwerken des Forschungsverbunds definiert. Entsprechend der in Kapitel 6.7 aufgeführten Kriterien der Verhältnismäßigkeit kann in bestimmten Fällen von der administrativen Trennung auch abgesehen werden.

In der Studiendatenbank wird im Regelfall auch eine Information über die datenliefernde Stelle als Teil des medizinischen Datensatzes (MDAT) gespeichert. Somit wird die Herkunft eines Datensatzes in Bezug auf den Arzt oder Prüfer sowohl als Teil der MDAT in der Studiendatenbank wie auch als Teil der $OrgDAT_{PL}$ in der Patientenliste gespeichert. Dies ist unproblematisch, solange je datenliefernder Stelle oder je Zentrum eine ausreichend große Zahl an Probanden rekrutiert wird und eine Reidentifikation aufgrund der Kenntnis der Einrichtung ausgeschlossen werden kann. Wenn jedoch die Angabe der behandelnden Einrichtung ein nennenswertes Reidentifizierungsrisiko darstellt, muss diese Information aus dem MDAT-Datensatz entfernt werden und darf nur noch als $OrgDAT_{PL}$ als Teil der Angaben in der Patientenliste hinterlegt sein. Die doppelte Speicherung der datenliefernden Stelle bzw. der behandelnden Einrichtung führt zu einer vereinfachten Abbildung der Prozesse zur Qualitätssicherung und des Rückfragemanagements, wie auch des Monitorings und des Managements unerwarteter Ereignisse. Für diese Prozesse ist eine Beteiligung der Patientenliste dann nicht mehr notwendig. Hierfür kann jeweils eine direkte Kommunikation zwischen der Studiendatenbank und den datenliefernden Stellen genutzt werden.

Nach Abschluss des Forschungsprojekts oder der Studie sind die Daten der Studiendatenbank und der Patientenliste zu anonymisieren oder zu löschen, sofern keine Zusammenführung in zweifach pseudonymisierter Form in einer Forschungsdatenbank entsprechend der in Kapitel 6.4 beschriebenen Form geplant ist. Unabhängig von der weiteren Verarbeitung oder Löschung der Daten in der Studiendatenbank müssen ggf. die gesetzlichen Aufbewahrungspflichten, z.B. für klinische Studien gemäß AMG, berücksichtigt werden. Dies kann bedeuten, dass pseudonymisierte Daten weiterhin in einer Studienzentrale aufzubewahren sind, allerdings nicht mehr im direkten Zugriff der Forscher. Der Zugriff auf die archivierten Daten ist entsprechend zu regeln.

5.2.3.2 Variante ohne zentrale Patientenliste

In bestimmten Fällen wird eine zentrale Patientenliste entweder nicht benötigt oder nicht umsetzbar sein. Insbesondere wenn Patienten mit hoher Wahr-

scheinlichkeit nur in ein einziges Forschungsprojekt eingeschlossen werden und die Daten eines Patienten nur in genau einer Einrichtung erhoben werden, kann eine lokale Erzeugung von Pseudonymen je Einrichtung ausreichend sein. Allerdings ist zu beachten, dass eine Kontaktaufnahme mit den Patienten nicht mehr möglich ist, wenn die behandelnde Einrichtung diese nicht mehr vermitteln kann. Problematisch kann eine Umsetzung einer zentralen Patientenliste sein, wenn allein aus dem Vorhandensein eines IDAT-Datensatzes in der zentralen Datei Rückschlüsse auf eine z.B. stigmatisierende Erkrankung gezogen werden können. Insofern enthalten die IDAT im Regelfall indirekt auch ein medizinisches Datum wie z.B. die Diagnose. Eine zentrale Patientenliste wird im Regelfall nicht beschlagnahmesicher organisiert werden können, auch dann nicht, wenn ein Notar mit der Führung und Administration beauftragt wird (s. Kap. 4.2.5). Dies kann für bestimmte Patientengruppen eine zentrale Patientenliste so unattraktiv machen, dass ausreichende Rekrutierungsraten verhindert werden.

Ohne eine zentrale Patientenliste und damit im Regelfall auch ohne eine zentrale treuhänderische Verwaltung der Einwilligungserklärungen, werden die Einwilligungserklärungen und die identifizierenden Daten in den behandelnden Einrichtungen verbleiben. Es ist im Regelfall zu empfehlen, eine lokale Patientenliste anzulegen und sicher aufzubewahren, da dies im Falle von Nachfragen zu einem deutlich schnelleren Auffinden der nötigen Unterlagen führt. Die Verantwortlichkeiten für die lokale Patientenliste sind klar zu definieren und festzulegen.

In der Studiendatenbank ist in diesem Falle immer die datenliefernde Stelle zu vermerken. Die dadurch entstehenden potenziellen Reidentifikationsrisiken bei Zentren mit sehr geringen Rekrutierungszahlen sind zu berücksichtigen. Die Kommunikation zwischen Studiendatenbank und datenliefernden Stellen ist, von dieser Notwendigkeit abgesehen, analog zu der Variante mit zentraler Patientenliste konzipierbar.

5.2.3.3 Identität von Sponsor und Prüfer

Vornehmlich wissenschaftlich motivierte Arzneimittelstudien, so genannte Investigator Initiated Trials (IIT), unterliegen seit der 12. Novellierung des Arzneimittelrechts denselben Regularien wie die industriell gesponsorten Studien im Vorfeld einer Zulassung. Damit gilt auch hier das im AMG vorgeschriebene Pseudonymisierungsgebot bei Weiterleitung von Daten an den Sponsor. Wenn jedoch in einer monozentrischen Studie an einem Universitätsklinikum die Rollen des Sponsors und Prüfers zusammenfallen, ist eine durchgängige Pseudonymisierung gegenüber den im Behandlungsverhältnis stehenden Prüfärzten als Angestellten des Sponsors verzichtbar. Weitere Informationen zu diesem Spezialfall finden sich in Kapitel 4.3.1 zu den ethischen und rechtlichen Grundlagen.

5.2.4 Nutzer, Rollen und Rechte

Für die Patientenliste wird ein Administrator und ggf. eine Dokumentationskraft zur Unterstützung benötigt. Diese haben vollen Zugriff auf den IDAT-Datensatz und sind entsprechend zum datenschutzgerechten Umgang mit diesen Daten zu verpflichten. Insbesondere müssen sie bei Depseudonymisierungsanfragen die identifizierenden Daten zu den jeweiligen Pseudonymen herausgeben, wenn dies von dem hierfür zuständigen Gremium angeordnet wird. Solche Gremien, für die die Bezeichnung „Ausschuss Datenschutz" benutzt wird, werden ausführlicher in dem Kapitel 5.2.5 zu den Verantwortlichkeiten und bei den organisatorischen Regelungen in Kapitel 6.6 beschrieben.

Für die Studiendatenbank ist ebenfalls administratives Personal notwendig. Zudem sind hier die Mitarbeiter des zentralen Datenmanagements anzusiedeln, die Zugriff auf die Daten aller Probanden in der Studiendatenbank haben.

Die Studienärzte oder Dokumentationskräfte in den behandelnden Einrichtungen sollten nur die Daten ihrer Probanden sehen. Dies ist auch bei einem Electronic Capture System (EDC) – oft auch als Remote Data Entry System (RDE) bezeichnet – umzusetzen, in dem sowohl die Probanden, als auch die Prüfer jeweils genau einer datenliefernden Stelle zugeordnet werden.

Vermehrt werden auch Patienten selbst in die Dokumentationsabläufe eingebunden. So sind z.B. bei Forschungsprojekten zum Thema „Schmerzen" zunehmend „Schmerztagebücher" durch die Patienten selbst zu führen. Hintergrund dessen ist unter anderem die schon länger bekannte aber erst in der jüngeren Vergangenheit vermehrt diskutierte Unsicherheit retrospektiver Auskünfte von Patienten bei dem gleichzeitigen Wunsch nach möglichst relevanten und validen Endpunkten [vgl. z.B. 32]. Solche Funktionen können effektiv auch durch EDC-Systeme unterstützt werden, wobei dann sichergestellt werden muss, dass die Patienten nur jeweils auf ihre eigenen Daten zugreifen können. Zudem ist darauf zu achten, dass eine potenziell unsichere Systemumgebung beim Zugriff durch Patienten nicht die Sicherheit des Gesamtsystems gefährden darf.

In klinischen Studien, in denen eine bestimmte Datenqualität vorgeschrieben ist, werden Monitore eingesetzt, die die eingegebenen Daten auf Plausibilität und ggf. Übereinstimmung mit den Quelldaten überprüfen. Diese müssen sowohl Zugang zu den von ihnen zu überprüfenden zentralen Patientendaten, wie auch zu den Quelldaten in den beteiligten Zentren und behandelnden Einrichtungen haben. Da dieser Nutzerkreis außerhalb des Behandlungsverhältnisses steht und gleichzeitig auch Zugriff auf nicht pseudonymisierte Unterlagen hat, müssen Patienten entsprechend darüber aufgeklärt werden und darin einwilligen. Eine klare Verpflichtung aller Beteiligten auf einen datenschutzgerechten Umgang mit den Daten ist unerlässlich.

Im Rahmen klinischer Prüfungen nach AMG ist eine definierte Sponsorschaft Voraussetzung für die Zulassung der Studie. Ergänzend zu den Regelungen

für die Nutzer im Studienzentrum können auch besondere Zugriffsregeln an eine Sponsorrolle gebunden sein. Dies hängt davon ab, welche Aufgaben des Sponsors an die Studienzentrale delegiert werden. Einzelne Aufgabenfelder wie das SAE-Management oder die Archivierung der Daten können vom Sponsor an die Studienzentrale delegiert oder auch selbst übernommen werden. Entsprechend muss das Rollen- und Rechtesystem die Aufgabenverteilung abbilden können.

5.2.5 Verantwortlichkeiten

In einem Studienmodul ist möglicherweise die Verantwortlichkeit für die Durchführung einer einzelnen Studie von der Verantwortlichkeit für die Infrastruktur und das Studienmodul insgesamt zu trennen. Beide Verantwortlichkeiten, auch wenn sie von derselben juristischen Person übernommen werden, sollten klar geregelt und transparent dargestellt werden. Auf der Ebene einer einzelnen Studie ist ggf. auch die gesetzlich vorgeschriebene Verantwortlichkeit eines Sponsors festzulegen, wenn die Studie in den Anwendungsbereich des AMG oder MPG fällt. Wichtig ist die Festlegung einer übergeordneten Verantwortlichkeit dann, wenn die Daten nach der Beendigung einer Studie weiterhin pseudonymisiert vorgehalten und genutzt werden sollen (vgl. Kap. 6.4) oder wenn eine Studieninfrastruktur rechtlich unabhängig von einem oder mehreren Sponsoren einzelner Studien betrieben wird.

Die Gesamtverantwortung für das Studienmodul wird im Regelfall in der Studienzentrale liegen, die ggf. eine externe Einrichtung mit dem Aufbau und Management der Patientenliste beauftragt. Allerdings sind bei einer Einbettung des Studienmoduls in eine übergreifende Forschungsinfrastruktur auch andere Verantwortlichkeiten denkbar. So könnte die zentrale Verantwortlichkeit auch bei der Netzwerkzentrale eines übergeordneten Forschungsverbunds angesiedelt sein, insbesondere dann, wenn diese ggf. wechselnde Studienzentralen mit der Durchführung von Forschungsprojekten beauftragt.

In jedem Falle ist eine klare Benennung der Verantwortlichkeiten vorzunehmen. Insbesondere wird die Einrichtung eines zentralen Gremiums vorgeschlagen, welches über datenschutzrechtlich sensible Fragen, wie z.B. solche der Depseudonymisierung, zu entscheiden hat. Hierfür wird der Begriff „Ausschuss Datenschutz“ verwendet. Eine solche zentrale Einrichtung sollte zudem die Richtlinien und Policies im Umgang mit den Daten vorgeben.

Die Patientenliste ist der sensibelste Teil des Identitäts-Managements und ist damit, wenn sie zentral geführt wird, ein besonders schützenswerter Bereich. Datenschutzrechtlich ist zu berücksichtigen, dass die IDAT, obwohl sie in der Patientenliste nicht mit medizinischen Daten (MDAT) kombiniert werden, den betroffenen Personenkreis als Patienten eines Forschungsnetzes mit einem umschriebenen Krankheitsspektrum ausweisen können. Im Falle eines stigmatisierenden oder in anderer Hinsicht besonders sensiblen Krankheits-

bereichs ist daher eine auch in den Augen der betroffenen Patienten besonders vertrauenswürdige Stelle mit der Führung der Patientenliste zu beauftragen.

Die Studiendatenbank mit den medizinischen Daten (MDAT) und ggf. organisatorischen Daten unterliegt der Verantwortlichkeit der Leitungsebene der Studienzentrale bzw. den von dieser hierfür benannten Verantwortlichen. Die Verantwortlichkeit hierfür kann zudem in übergreifenden Forschungsinfrastrukturen in übergeordnete Verantwortlichkeiten eingebettet sein.

Nicht zu vergessen sind notwendige Regeln und Verantwortlichkeiten in den beteiligten Einrichtungen, in denen die Patienten untersucht und Daten erhoben werden. Wenn die Dateneingabe mittels EDC direkt in ein zentrales System erfolgt, sind auch Regeln für den Umgang mit den Zugangskriterien (z.B. Passwörter, PINs oder Chipkarten) zu definieren und einzuhalten. Hierfür müssen Verantwortliche in den beteiligten Einrichtungen festgelegt werden. Gleiches gilt für den Umgang mit einer lokalen Patientenliste, die üblicherweise ergänzend zu einer zentralen Liste geführt wird.

Wenn die Verantwortung für die Durchführung einer Studie bei einer vom Studienmodul rechtlich unabhängigen Stelle liegt, z.B. einem Sponsor gemäß AMG oder MPG, so hat dieser das Studienmodul bzw. einzelne Stellen wie die Studienzentrale oder an der Studie teilnehmende Zentren mit der Durchführung der relevanten Teilaufgaben zu beauftragen. Verantwortlichkeiten für Teilaufgaben wie z.B. die Datenerfasssung oder auch die Archivierung von Studiendaten können delegiert werden. Dabei hat ein Sponsor gemäß AMG jedoch die Pflicht, sich von der Eignung aller Beauftragten hinsichtlich einer GCP-konformen Durchführung einer Studie zu überzeugen und dies in ausreichendem Maße zu kontrollieren. Weitere Hinweise zur Sponsorschaft in klinischen Prüfungen nach der 12. AMG-Novelle können einem Kurzgutachten der Kanzlei Sträter entnommen werden [33].

5.2.6 Aspekte der Realisierung

Für die IT-Unterstützung klinischer Studien ist im Regelfall die Verwendung eines Studiensoftwaresystems empfehlenswert, welches z.B. die Definition elektronischer Eingabeformulare (Electronic Case Report Forms, eCRF) erlaubt, die von den beteiligten Einrichtungen für eine dezentrale Dateneingabe (Electronic Data Capture, EDC) genutzt werden können. Aus Datenschutzsicht ist entscheidend, dass solche Systeme eine verschlüsselte Übertragung der Daten (SSL) garantieren und zudem sicherstellen, dass keine identifizierenden Daten in direktem Zusammenhang mit medizinischen Daten erfasst und an den zentralen Server übermittelt werden. Zudem sollte gewährleistet sein, dass die Mitarbeiter eines beteiligten Zentrums nur die Daten „ihrer" Patienten einsehen und verändern können. Wenn Patienten in die Dokumentation derart eingebunden werden, dass sie auch einen Zugang zu dem Softwaresystem bekommen, muss darüber hinaus sichergestellt sein, dass jeder Patient nur seine eigenen Daten sieht und ggf. bearbeiten kann.

Solche Softwaresysteme bieten im Regelfall auch eine Funktion für die Erzeugung pseudonymer IDs (als Subject Identification Code, SIC), so dass für die Durchführung einzelner Studien ggf. kein zusätzliches Pseudonymisierungstool benötigt wird. Zu berücksichtigen ist allerdings, dass häufig keine zentrale Speicherung und Verwaltung der identifizierenden Daten mit angeboten wird. Eine Reidentifizierung eines Patienten ist dann nur mit Hilfe der dezentralen Listen in den beteiligten Einrichtungen oder bei manueller Durchsicht der ggf. zentral hinterlegten Einwilligungserklärungen möglich. Spätestens wenn ein übergeordnetes ID-Management benötigt wird, z.B. für die Zuordnung von Datensätzen eines Patienten aus mehreren Studien zueinander oder bei Beteiligung mehrerer Softwaresysteme mit unterschiedlichen Pseudonymisierungsvorgaben oder -funktionen, reichen die Funktionen dieser Softwaresysteme üblicherweise nicht mehr aus. In diesen Fällen empfiehlt sich die Verwendung einer hierfür spezialisierten Softwarekomponente, wie z.B. des PID-Generators der TMF. Eine solche Software hat die Aufgabe, entweder für jede einzelne Studie einen SIC entgegenzunehmen und zusammen mit den IDAT zu verwalten oder jeweils einen SIC auf Basis der IDAT selbst zu erzeugen und herauszugeben. Ein übergeordnetes ID-Management erfordert darüber hinaus die Zuordnung mehrerer SICs zu einem Patienten über ein übergeordnetes Pseudonym, den PID_S. Die Nutzung eines PID_S für eine dauerhafte Zusammenführung von Daten aus mehreren einzelnen Forschungsprojekten oder Studien ist in Kapitel 6.4 beschrieben.

Für die Nutzung in klinischen Studien nach AMG entsprechen fertig entwickelte Softwaresysteme üblicherweise hinsichtlich Funktionsumfang, Qualitätssicherung und Dokumentation den umfangreichen gesetzlichen Vorgaben bzw. den Kriterien der Good Clinical Practice (GCP). Hierzu gehört z.B. die Funktion eines umfassenden Audit-Trails, in dem alle Änderungen an Datensätzen nachvollziehbar gespeichert werden. Eigenentwicklungen oder nicht für AMG-Studien konzipierte Systeme genügen solchen Anforderungen häufig nicht. Bei Nutzung einer zusätzlichen Softwarekomponente für das zentrale ID-Management ist zu beachten, dass letzteres entsprechend den gesetzlichen Vorgaben und internationalen Regularien nur dann zu validieren ist, wenn die Softwarekomponente in das ID-Management einer einzelnen Studie eingreift. Wenn das zentrale ID-Management hingegen im Rahmen einer Studie nur vom validierten Studiensoftwaresystem generierte SICs entgegennimmt und diese nur für studienübergreifende Zwecke, wie z.B. Metaanalysen, wieder herausgibt, dann kann eine Validierung gemäß GCP für die Softwarekomponente des zentralen ID-Managements entfallen.

5.3 Forschungsmodul

Das Forschungsmodul stellt die Adaption des Modells B des bisherigen generischen Datenschutzkonzepts der TMF dar; die Einordnung in die übergeordneten Strukturen ist in Kapitel 6.1.7 beschrieben.

Die Bezeichnung als „Forschungsmodul“ bedeutet *nicht*, dass in den anderen Modulen keine Forschung stattfindet, sondern bezieht sich auf das Charakteristikum, dass hier die Forschung vom direkten klinischen Bezug entkoppelt und insbesondere nicht mit der direkten Krankenversorgung verzahnt ist. Das Forschungsmodul sieht zudem primär keine eigene Datenerfassung vor, sondern übernimmt Daten aus einem Klinischen (vgl. Kap. 5.1) oder Studien-Modul (vgl. Kap. 5.2) oder einer anderen geeigneten Datenquelle.

Ein Forschungsmodul kapselt eine oder mehrere Forschungsdatenbanken mit der dazu nötigen Infrastruktur. Es können beispielsweise unterschiedliche Datentypen zu einem Patienten (z.B. Bilder, genetische Daten etc.) in unterschiedlichen Datenbanken abgelegt sein, auf die über das Forschungsmodul zugegriffen werden kann.

5.3.1 Zweck und Anwendungsbereich

Das Forschungsmodul dient dazu, medizinische Daten hoher Qualität langfristig – auch für zukünftige Forschungsprojekte – zur Verfügung zu stellen. Daraus ergibt sich, dass der Verwendungszweck sowie die Lebensdauer der Daten weniger konkret angegeben werden können, als dies für das Studienmodul, wie es in Kapitel 5.2 beschrieben ist, gilt. Die Einsatzmöglichkeiten eines Forschungsmoduls sind sehr weit gefasst. Dies können gesundheitsökonomische oder epidemiologische Studien sein, aber auch die Ermittlung von Fallzahlen bzw. von Patienten für klinische Studien kann ermöglicht werden. Im Gegensatz zum Klinischen Modul ist ein unmittelbarer Behandlungsbezug der gespeicherten Daten nicht notwendigerweise gegeben. Mit Hilfe eines Forschungsmoduls können große Kollektive abgebildet werden, die über einen längeren Zeitraum beobachtet werden, ohne dass die Vertraulichkeit der Information angetastet wird. Eine direkte Verknüpfung der Identitätsdaten mit den medizinischen Daten einer Forschungsdatenbank ist generell ausgeschlossen, da kein zur unmittelbaren Identifikation eines Patienten führendes Merkmal – wie z.B. der PID des Klinischen Moduls – als Ordnungskriterium in einer Forschungsdatenbank geführt wird. Das Forschungsmodul kann medizinische Daten zu einem Patienten aus mehreren Studien oder Systemen verwalten und bietet Forschern somit einen Datenpool, der sich zur Generierung neuer Fragestellungen oder für Sekundärauswertungen eignet.

Die medizinischen Daten des Forschungsmoduls können potenziell nicht nur den Forschern, die direkt an einer Studie beteiligt sind, zur Verfügung gestellt werden, sondern auch anderen Forschern eines Forschungsverbundes, externen Forschern oder auch der Industrie.

Je nach Aufbau des Forschungsmoduls bzw. abhängig von den Regularien eines Forschungsverbundes wird den Forschern ein direkter Zugang auf die Daten in den Datenbanken gewährt oder ein Export der Daten übermittelt. Bei einem direkten Zugriff auf die Forschungsdatenbanken können für die Sekundär-

nutzung von Daten aus der klinischen Forschung komfortable Such-, Filter- und Selektionsmechanismen zur Verfügung gestellt werden.

5.3.2 Anwendungsfälle

5.3.2.1 Probanden in das Forschungsmodul aufnehmen

Anders als bei der Aufnahme in andere Module eines Forschungsverbunds wird die Aufnahme in das Forschungsmodul im Regelfall nicht interaktiv und im Kontakt zum betroffenen Probanden oder Patienten stattfinden. Allerdings setzt auch die Übermittlung eines personenbezogenen Datensatzes in das Forschungsmodul eine informierte Einwilligung des Betroffenen (vgl. Kap. 3.2.3.1) voraus. Daher ist das Vorliegen einer ausreichenden Einwilligung, die zudem die typischerweise mit der Übermittlung in das Forschungsmodul einhergehende Zweckänderung und Langfristigkeit der Speicherung abdeckt, vor der Übermittlung zu prüfen.

5.3.2.2 Datenqualität sichern

Wird das Forschungsmodul mit anderen Modulen (z.B. dem Studienmodul oder Klinischen Modul) gekoppelt, so können schon vorhandene Daten eines Patienten aus dem Forschungsmodul zum Zwecke der Qualitätssicherung genutzt werden. Eine genaue Beschreibung befindet sich im Kapitel 6.3 zum kombinierten Einsatz von Studien- und Forschungsmodul.

5.3.2.3 Daten mit externen Quellen abgleichen

Im Zuge eines Forschungsvorhabens können neben dem Datenbestand der Forschungsdatenbank auch Informationen aus externen Datenquellen z.B. dem Melderegister oder Daten der Gesundheitsämter herangezogen werden. Dies können beispielsweise Anfragen an die Einwohnermeldeämter sein, ob die in einem Forschungsvorhaben betrachteten Personen noch leben. Bei einem Datenabgleich sind die datenschutzrechtlichen Bestimmungen der datenliefernden Stelle zu berücksichtigen. Zusätzlich muss der Datenabgleich durch das Forschungsvorhaben gut begründet sein. Gegebenenfalls muss entschieden werden, ob das Interesse der Allgemeinheit an diesem Forschungsvorhaben das Recht der einzelnen Person auf informationelle Selbstbestimmung überwiegt. Auf die rechtlichen Rahmenbedingungen zum Abgleich mit externen Datenbeständen wird im Kapitel 4.3.4 genauer eingegangen.

5.3.2.4 Machbarkeit einer Studie prüfen

Um die Machbarkeit einer Studie prüfen zu können, müssen Indizien dazu ausgewertet werden, wie viele den spezifizierten Ein- und Ausschlusskriterien entsprechende Patienten innerhalb einer bestimmten Zeitspanne zu erwarten sind. Die Information, ob die Patienten eingewilligt haben, über weitere Stu-

dien informiert zu werden, kann bei der Machbarkeitsprüfung einer Studie ggf. mit berücksichtigt werden.

Die Machbarkeitsprüfung einer Studie auf Grundlage der Daten des Forschungsmoduls, kann durch drei unterschiedliche Verfahren realisiert werden:

- Der Forscher erhält direkten Zugriff auf die Forschungsdatenbank und kann durch Abfragen der Ein- und Ausschlusskriterien entsprechend aggregierte Informationen über das zu erwartende Patientenkollektiv bekommen.
- Der Forscher erhält einen Export und verfährt dann wie bei (1).
- Der Betreiber bzw. Verantwortliche der Forschungsdatenbank erhält bestimmte Anfragen eines Forschers (z.B. die Ein- und Ausschlusskriterien einer Studie) und liefert dem Forscher als Ergebnis eine Anzahl geeigneter Patienten zurück.

Bei diesen Abfragen müssen geeignete Mechanismen verhindern, dass einzelne Patienten durch gezieltes Abfragen identifiziert werden können. Z.B. kann bei Abfragen, die eine bestimmte Anzahl von Patienten unterschreiten, nicht mehr die genaue Patientenanzahl ausgegeben werden, sondern nur noch der Hinweis, dass das Mindestmaß an Patienten unterschritten ist. Bei einer Datenbereitstellung als Export müssen geeignete Maßnahmen zur Anonymisierung der Rohdaten getroffen werden (vgl. Kap. 5.3.2.9).

5.3.2.5 Rekrutierung unterstützen

Patienten, die bereits an einem früheren Forschungsprojekt teilgenommen haben, können mit Hilfe des Forschungsmoduls auch effektiv für weitere Studien rekrutiert werden. Dies kann insbesondere bei chronischen Erkrankungen von Interesse sein. Anders als bei der Überprüfung der Machbarkeit wird hierfür eine Depseudonymisierung der Datensätze ausgelöst werden müssen, die den gesuchten Ein- und Ausschlusskriterien entsprechen. Das Verfahren der Depseudonymisierung wird im Kapitel 6.1 zum Identitätsmanagement genauer beschrieben. Idealerweise sollten die hinterlegten Einwilligungserklärungen der ausgewählten Patienten eine direkte Ansprache aus dem Forschungsverbund heraus erlauben. Andernfalls könnte auch eine Ansprache über die aktuell behandelnde Einrichtung geregelt sein.

5.3.2.6 Auskunft geben

Wünscht ein Patient Auskunft über die in dem Forschungsmodul über ihn gespeicherten Daten, wird die Auskunftserteilung in geeigneter Form geprüft und über das Identitätsmanagement an das Forschungsmodul weitergeleitet. Im Forschungsmodul werden die medizinischen Daten des Patienten ggf. aus mehreren Datenbanken selektiert und an das Identitätsmanagement zurückgeschickt. Bei diesem Vorgang muss durch geeignete Mechanismen verhindert werden, dass das im Forschungsmodul verwendete Pseudonym (PSN) des Pa-

tienten Unbefugten offenbart wird (s. hierzu Kap. 6.1 Identitätsmanagement und Kap. 6.4 Studienmodul und Forschungsmodul).

5.3.2.7 Daten auswerten

Die Daten des Forschungsmoduls können, je nach Aufbau der Infrastruktur und der organisatorischen Regelungen, sowohl im Sinne einer Erstauswertung (z.B. bei epidemiologischen Registern) als auch im Rahmen einer Sekundärauswertung (z.B. für eine retrospektive Studie) genutzt werden. Die Zugriffe auf die Daten können online oder auch in Form eines Exports erfolgen.

5.3.2.8 Daten an Forscher weitergeben (auf Basis einer Einwilligung)

Bei Vorliegen einer entsprechenden Einwilligung kann einem Forscher nach Antrag und entsprechender Bewilligung ein direkter Zugriff auf einen bestimmten Ausschnitt (z.B. eine Studie) des Forschungsmoduls gewährt werden. Alternativ werden die entsprechenden Daten als Export bereitgestellt. Die Einwilligung für die Weitergabe für ein bestimmtes Forschungsprojekt kann zum Zeitpunkt der Datenerhebung durch eine den Zweck des Forschungsprojekts mit umfassende Formulierung erfolgt sein, ggf. auch im Rahmen einer abgestuften Einwilligung (vgl. Kap. 4.2.2). Alternativ kann in bestimmten Fällen auch die spätere Einholung einer separaten Einwilligung für ein konkretes Forschungsprojekt möglich und nötig sein.

Bei einem direkten Zugriff auf die Datenbank muss sichergestellt sein, dass die Summe der zu einem Patienten verfügbar gemachten medizinischen Daten (ggf. aus mehreren Datenbanken zusammengeführt) nicht zu einem relevanten Reidentifizierungsrisiko führt. Zudem sollte das als dauerhaftes Ordnungskriterium in der Datenbank genutzte Pseudonym den zugreifenden Forschern verborgen bleiben.

Wenn Daten des Forschungsmoduls in Form eines Exports für weitere Auswertungen benötigt werden, muss der hierfür zuständige Wissenschaftler einen entsprechenden Antrag auf einen Datenexport stellen. Hierfür ist zu spezifizieren, welche Daten benötigt werden und ob im Rahmen der Auswertung möglicherweise mit relevanten Ergebnissen für einzelne Patienten zu rechnen ist und eine solche Rückmeldung im Vorfeld vereinbart wurde. Wenn keine relevante individuelle Rückmeldung der Ergebnisse an die Patienten zu erwarten ist, werden die Daten für den Export anonymisiert, andernfalls werden die Daten mit einem neuen Pseudonym versehen und exportiert. Wenn Daten aus mehreren Forschungsdatenbanken innerhalb des Forschungsmoduls für eine Auswertung zusammengeführt werden, muss sichergestellt sein, dass dadurch keine Reidentifizierung des Patienten ermöglicht wird. Sowohl bei anonymisierten wie auch pseudonymisierten Exporten ist darauf zu achten, dass sich die Sortierreihenfolge der exportierten Datensätze nicht nach dem langfristigen Pseudonym PSN im Forschungsmodul

richtet, sondern z.B. nach den neu erzeugten anonymen oder pseudonymen IDs.

5.3.2.9 Daten an Forscher weitergeben (unabhängig von einer Einwilligung)

Externen Forschern, für deren Zugriff keine Einwilligung der Probanden vorliegt, können Daten in Form eines Online-Zugriffes sowie als Export zur Verfügung gestellt werden. Das Vorgehen bei den Zugriffen auf die Forschungsdaten für externe Forscher ist angelehnt an die Regelungen der Forschungsdatenzentren der statistischen Ämter des Bundes und der Länder[22]. Daraus ergibt sich, dass für externe Forscher der Zugriff auf die Daten des Forschungsmoduls in der Regel faktisch anonymisiert erfolgen kann.

Bei einem Online-Zugriff werden zwei Möglichkeiten vorgeschlagen, die beide ein möglichst geringes Reidentifizierungsrisiko für die Patienten mit sich bringen:

- Den Forschern werden spezielle PC-Arbeitsplätze bereitgestellt an denen sie arbeiten können. Bei diesen Arbeitsplätzen gibt es eine spezielle Regulierung des Datenzugangs, die die Reidentifizierung des Patienten verhindert. Durch diese Mechanismen können den externen Forschern die Daten faktisch anonymisiert zur Verfügung gestellt werden.
- Die Forscher bekommen Zugriff auf Dummy-Daten, die in Aufbau und Merkmalsausprägungen dem Originalmaterial gleichen. Mit Hilfe dieser Dummy-Dateien können die Forscher, entsprechend ihrer Fragestellung, spezielle Abfragen erstellen. Diese Abfragen werden anschließend von den Verantwortlichen für die Forschungsdatenbank (z.B. Biometrie-Einheit) auf den Originaldaten angewendet. Die Forscher erhalten nach einer notwendigen Geheimhaltungsprüfung schließlich die Ergebnisse dieser Auswertung. Dieses Vorgehen ermöglicht die Arbeit mit absolut anonymisierten Daten.

Neben dem Online-Zugriff können externen Forschern auch absolute bzw. faktisch anonymisierte Exporte zur Verfügung gestellt werden. Bei den faktisch anonymisierten Exporten handelt es sich um sogenannte Scientific-Use-Files, die wissenschaftlichen Institutionen zur Verfügung gestellt werden. Vertragliche Vereinbarungen zur Nutzung und Weitergabe der Daten können ein evtl. noch vorhandenes Reidentifizierungsrisiko begrenzen. Für die Bereitstellung von Daten für die breite Öffentlichkeit können absolut anonymisierte Exporte (Public-Use-Files) bereitgestellt werden, die nur ausgewählte oder vergröberte Merkmale enthalten. Um ein Reidentifizierungsrisiko für die einzelnen Patienten auszuschließen, sollte bei der Auswahl der Merkmale das Prinzip der k-Anonymität berücksichtigt werden, wobei die Größe von k geeignet zu wählen ist. Auch bei diesen Exporten ist auf eine Sortierung unab-

22 http://www.forschungsdatenzentrum.de/datenzugang.asp

hängig vom langfristig genutzten Pseudonym zu achten [34]. Weitere Hinweise und Hilfestellungen für die Bereitstellung anonymer Daten, gerade auch in internationalen Projekten, finden sich in [35].

5.3.2.10 Ergebnisse mitteilen

Im Falle, dass ein Patient über Forschungsergebnisse benachrichtigt werden soll, ist dieser Vorgang in jedem Einzelfall von Antrag und Bewilligung durch den Ausschuss Datenschutz des Forschungsverbundes abhängig. Das Verfahren ist so einzurichten, dass es erst nach aktueller Prüfung der Genehmigung durch den Verantwortlichen manuell gestartet werden kann. In diesen Fällen geht der Vorgang von der Forschungsdatenbank aus. Die Identifizierung und Benachrichtigung des Patienten über das Identitätsmanagement erfolgt analog zu dem Verfahren, wie es beim Erteilen der Auskunft vorgesehen ist (s.a. Kap. 6.1.2 zur Mitteilung von Ergebnissen).

5.3.3 Daten und Datenflüsse

Die Forschungsdatenbanken des Forschungsmoduls enthalten ausschließlich medizinische Daten, die mit einem Pseudonym (PSN) versehen sind, das außerhalb des Forschungsmoduls nicht offenbart werden darf. Neben den Administratoren können zusätzlich speziell autorisierte Services, die mit dem Identitätsmanagement kommunizieren, auf die Forschungsdatenbanken des Forschungsmoduls zugreifen (s.a. Kap. 6.1.6.2).

Aus den oben genannten Anwendungsfällen lassen sich folgende Datenflüsse in Bezug auf die Forschungsdatenbanken des Forschungsmoduls ableiten:

5.3.3.1 Transfer medizinischer Daten in eine Forschungsdatenbank

Bevor medizinische Daten eines Patienten in eine Forschungsdatenbank eines Forschungsverbundes transferiert und dort gespeichert werden können, ist sicherzustellen, dass diese mit einem Pseudonym (PSN) versehen werden, das an keiner Stelle zusammen mit identifizierenden Daten des Patienten gespeichert werden darf. Somit wird eine eindeutige Zuordnung der Daten zum richtigen Patienten vor der Pseudonymisierung vorausgesetzt. Dies ist eine Aufgabe des im Kapitel 6.1 beschriebenen Identitätsmanagements.

Das Pseudonym wird von einer für das Identitätsmanagement legitimierten Institution des Forschungsverbundes erzeugt und zusammen mit den medizinischen Daten an eine Forschungsdatenbank weitergeleitet. Dort dient das PSN als Zuordnungskriterium für die Speicherung und die Zusammenführung der Daten und für alle fallbezogenen Auswertungen, die daraus abgeleitet werden. Die Kennungen der medizinischen Einrichtungen oder der individuellen Ärzte – so genannte organisatorische Daten (OrgDAT), wie sie im Kapitel zum Maximalmodell (s. Kap. 6.5) beschrieben sind – können in den For-

schungsdaten im Klartext oder ebenfalls pseudonymisiert gespeichert werden. Bei einer Speicherung solcher Daten im Klartext muss gewährleistet sein, dass hierdurch kein relevantes Reidentifizierungsrisiko für Patienten entsteht. Des Weiteren muss bei der Zusammenführung der medizinischen Daten eines Patienten aus verschiedenen Quellen in einer Datenbank (z.B. unterschiedlichen Studien) sichergestellt werden, dass durch diese Zusammenführung das Reidentifizierungsrisiko nicht zu groß wird.

Die medizinischen Daten können sowohl aus der direkten Versorgung (Klinisches Modul, Kap. 5.1), aus klinischen Studien (Studienmodul, Kap. 5.2) oder aus anderen Datenbanken (z.B. Registern) des Forschungsverbundes stammen oder auch direkt für das Forschungsmodul erfasst worden sein, wie z.B. Daten von Kontrollpersonen bei epidemiologischen Kohortenstudien. Sollten schon Daten zu einem PSN vorhanden sein, können diese zusammengeführt werden. Die Übertragung von Daten aus einer Studiendatenbank in eine Forschungsdatenbank wird im Kapitel 6.4 (Studien- und Forschungsmodul) detailliert beschrieben.

5.3.3.2 Ändern medizinischer Daten in einer Forschungsdatenbank

Es kann die Notwendigkeit bestehen, medizinische Daten, die sich schon in einer Forschungsdatenbank befinden, zu ändern. Dies kann z.B. im Rahmen einer Qualitätssicherung notwendig sein, wie sie im Kapitel 6.4 (Studien und Forschungsmodul) beschrieben wird. Es können aber auch bei der sekundären Auswertung Fehler entdeckt werden, die dann ebenfalls im Datenbestand des Forschungsmoduls geändert werden sollten. Für die Änderungen eines Datensatzes wird dieser anhand seines PSN selektiert und geändert bzw. überschrieben. Aus Sicht des Datenschutzes kann es dem Betreiber der Forschungsdatenbank überlassen werden, ob er die Änderung in Form einer Versionierung oder mit Hilfe eines Audit-Trails nachvollziehbar macht. Im Sinne einer hohen Datenqualität sind aber Funktionen, die eine Nachvollziehbarkeit aller Änderungen gewährleisten, auf jeden Fall zu empfehlen.

5.3.3.3 Anonymisieren bzw. Löschen medizinischer Daten in der Forschungsdatenbank

Ein Patient hat jederzeit das Recht, seine Einwilligungserklärung für die Speicherung medizinischer Daten im Rahmen eines Forschungsvorhabens zurückzuziehen. Des Weiteren dürfen medizinische Daten je nach Forschungsvorhaben nur für eine bestimmte Dauer in pseudonymisierter Form gespeichert werden; dies ist im Regelwerk des Forschungsverbunds zu definieren und muss durch die jeweilige Einwilligungserklärung abgedeckt sein. Ein weiterer Grund für die Anonymisierung bzw. Löschung der Daten eines Patienten ist dessen Versterben.

In diesen Fällen bedeutet dies für den Betreiber einer Forschungsdatenbank, dass er die medizinischen Daten eines Patienten anonymisieren oder löschen

können muss. Bei der Anonymisierung müssen die ggf. extern, z.B. in einer Patientenliste, gespeicherten identifizierenden Daten (IDAT) gelöscht und das Pseudonym als Ordnungskriterium in der Forschungsdatenbank durch eine anonyme Kennung ersetzt werden (s. Anwendungsfall Widerruf in Kap. 6.1.2). Bei der Erzeugung anonymer Kennungen ist zu beachten, dass diese nicht mit schon bestehenden anonymen oder pseudonymen Kennungen in der Forschungsdatenbank übereinstimmen dürfen. Das Löschen der Daten aus einer Forschungsdatenbank erfordert ebenso wie das Anonymisieren auch ein Löschen der ggf. extern gespeicherten IDAT. Die Anonymisierung kann im Einzelfall und nach Abschätzung des Reidentifizierungsrisikos auch erfordern, dass einzelne charakteristische Merkmale des Falls gelöscht oder vergröbert werden. Genauere Details, wie dies im Zusammenhang mit einem Identitätsmanagement erfolgen kann, sind im Kapitel 6.4 (Studien- und Forschungsmodul) beschrieben.

5.3.3.4 Austausch der Pseudonyme einer Forschungsdatenbank

Der Austausch der Pseudonyme einer Forschungsdatenbank kann aus unterschiedlichen Gründen notwendig werden: Z.B. bei Verlust oder Kompromittierung einer zur Pseudonymisierung genutzten SmartCard oder bei drohender Kompromittierung des verwendeten Verschlüsselungsalgorithmus. Liegt die Notwendigkeit eines Austausches der Pseudonyme vor, so muss dieser durch das Identitätsmanagement durchgeführt werden. Hierbei muss durch geeignete Verfahren sichergestellt werden, dass die neuen Pseudonyme dem richtigen Patienten bzw. Datensatz zugewiesen werden (Kap. 6.1.2 Umpseudonymisierung).

5.3.4 Nutzer, Rollen und Rechte

Der Zugriff auf die Forschungsdatenbank kann durch den Administrator sowie durch einen autorisierten internen bzw. externen Forscher erfolgen.

Der Administrator hat vollen Zugriff auf die Datenbank und kann entsprechende Selektionen und Exporte veranlassen.

Der interne Forscher kann seinem Antrag entsprechend bestimmte Teile der Forschungsdatenbank einsehen. Auch hier ist bei einem studienübergreifenden Zugang wieder das Reidentifizierungsrisiko der einzelnen Patienten abzuschätzen. Während der Administrator die PSN in der Forschungsdatenbank sehen darf, bleiben diese dem Forscher verborgen.

Der externe Forscher hat in der Regel nur anonymisierten Zugriff auf die Daten. Dieser kann sowohl online als auch in Form eines Exportes erfolgen.

Hat ein behandelnder Arzt auch in der Rolle eines Forschers Zugriff auf Daten eines seiner Patienten, so sollte sichergestellt werden, dass er diesem keine weiteren medizinischen Daten zuordnen kann, die ihm im Rahmen der Behandlung verborgen geblieben wären (z.B. genetische Informationen, s.a. Kap. 6.2.3.3).

5.3.5 Verantwortlichkeiten

Da ein Forschungsmodul der Bereitstellung von Daten für die Forschung über einen langen Zeitraum dient, muss auch die Verantwortlichkeit für die Datenverarbeitung langfristig geregelt und für die Patienten transparent dargestellt werden. Hierfür ist auch die Auswahl oder ggf. Etablierung einer rechtsfähigen Einrichtung bzw. eines Forschungsverbunds als juristischer Person notwendig. Der Zugriff auf die Daten der Forschungsdatenbank muss über den von der verantwortlichen Stelle eingerichteten Ausschuss Datenschutz bewilligt werden. Forscher erhalten ein Zugriffsrecht auf die Daten, wenn dies vom Ausschuss Datenschutz nach Prüfung des Forschungsansatzes und des dafür benötigten Datensatzes bewilligt wird.

Der Betrieb und die Administration des Forschungsmoduls sollten möglichst räumlich und organisatorisch getrennt von anderen Modulen, wie z.B. dem Identitätsmanagement, erfolgen. Für die Erstellung und Einhaltung der Regeln bezüglich des Umganges mit den Forschungsdaten bzw. der Kontaktierung des Patienten ist das Management des Forschungsverbundes zuständig bzw. ein vom Management beauftragter Dienstleister.

5.3.6 Aspekte der Realisierung

Im Gegensatz zu den Studiendatenbanken, die sich in den letzten Jahren immer mehr als „Standardprodukte" etabliert haben, gibt es relativ wenige IT-Lösungen für die Anforderungen einer Forschungsdatenbank. Mit dem Pseudonymisierungsdienst der TMF sind zwar schon die Anforderungen für das Identitätsmanagement (Pseudonymisierung, Depseudonymisierung, Findingmanagement etc.) abgedeckt, jedoch fehlt es noch an nationalen IT-Lösungen für die Umsetzung der oben beschriebenen Anwendungsfälle. Der Pseudonymisierungsdienst der TMF könnte auch eingesetzt werden, um Exporte aus einer Forschungsdatenbank mit projektindividuellen, bei Bedarf reidentifizierbaren Pseudonymen zu versehen (vgl. Kap. 6.1.1.2).

Als internationale Lösung wäre das Projekt I2B2 (Informatics for Integrating Biology and the Bedside) zu nennen [36]. I2B2 ist ein von der NIH gefördertes Projekt in den USA, welches u.a. ein Open Source Tool entwickelt, mit dem die Zusammenführung klinischer Datenbestände und die Abfrage medizinischer Datenbestände ermöglicht werden. Somit können u.a. Machbarkeitsanalysen für neue Studien realisiert werden.

Auch wenn das I2B2-Tool eine gute Grundlage für eine Forschungsdatenbank darstellt, sind noch einige Anpassungen bezüglich des Datenschutzes sowie einige Verbesserungen bezüglich der Funktionalität zu realisieren. Ein Punkt ist der Ausbau des Rechte- und Rollenmanagements (alle Nutzer können momentan den gesamten Datenbestand einsehen). Als weiterer Punkt ist der Im- und Export der Daten zu nennen. Hier bedarf es ebenfalls einiger Erwei-

terungen, da momentan noch keine Schnittstellen für gängige Datenstandards wie CDISC, HL7 etc. vorhanden sind. Im Rahmen eines TMF-Projekts[23] wurde 2012 jedoch ein Toolkit auf Basis der I2B2-Plattform und mit Hilfe einer frei verfügbaren Version der Software Talend Open Studio[24] erstellt, welches standardisierte Importe für eine Reihe von Formaten ermöglicht.

Für die Bereitstellung anonymer Exporte aus Forschungsdatenbanken stellt die TMF kostenfrei eine Softwarekomponente zur Verfügung, die vorhandene Daten in verschiedenen Formaten nach umfangreicher Parametrierung unter möglichst geringem Informationsverlust zuverlässig k-anonymisiert.[25]

5.4 Biobankenmodul

Für Biobanken (oder Biomaterialbanken) hat die TMF bereits die bisherigen generischen Datenschutzkonzepte aus dem Jahre 2003 erweitert und 2006 ein angepasstes und mit den Datenschützern auf nationaler Ebene abgestimmtes Datenschutzkonzept vorgestellt [2]. Dieses bleibt weiterhin gültig und ist nicht Gegenstand dieser Revision. Es ist dann einschlägig, wenn der Biobank-Betrieb der eigentliche Gegenstand eines Datenschutzkonzepts ist; seine Einordnung in die neue umfassende Struktur wird in Kapitel 6.1.7 beschrieben.

In diesem Kapitel werden die dortigen Ausführungen soweit wiederholt, wie es nötig ist, um die Einpassung von Biobanken in das modulare Konzept für medizinische Forschungsverbünde beschreiben zu können. Die Abgrenzung eines Biobankenmoduls von weiteren im Forschungsverbund existierenden Modulen spiegelt einerseits die technisch und organisatorisch unterschiedliche Handhabung von Biomaterialien wider, andererseits die besondere Sensibilität von genetischen Daten, die aus der Analyse der Materialien entstehen und in der Regel von anderen Daten getrennt gespeichert werden sollten.

5.4.1 Zweck und Anwendungsbereich

Ein Biobankenmodul enthält eine oder mehrere Probenbanken zusammen mit organisatorischen oder administrativen Daten (OrgDAT) zu den Proben oder Biomaterialien, die in einer direkt bei der Probenbank angesiedelten Datenbank verwaltet werden. Auch eine Datenbank für die aus den Proben gewonnenen Analysedaten (AnaDAT, im BMB-Konzept etwas missverständlich als ProbDAT bezeichnet) gehört in der Regel in das Biobankenmodul. Zu einer Biobank gehören immer auch Komponenten zum Identitätsmanagement (s. Kap. 6.1), die mehr oder weniger zentral betrieben werden, und eine Daten-

23 siehe www.tmf-ev.de/idrt
24 siehe www.talend.com
25 siehe www.tmf-ev.de/produkte/P100201

bank mit klinischen Annotationen, die im modularen Aufbau eines Verbunds im Forschungsmodul (s. Kap. 5.3) oder Klinischen Modul (s. Kap. 5.1) angesiedelt, also vom Typ her eine Klinische Datenbank (KDB) oder Forschungsdatenbank (FDB) ist; sie wird im Kontext dieses Kapitels als Annotationsdatenbank bezeichnet.

Aufgabe der Probenbank ist die Aufbewahrung von Proben. In der Regel ist sie an einem Labor oder einem biomedizinischen Institut angesiedelt. Die Probenbank erhält die Probe direkt von der Daten erhebenden Stelle bzw. von einem weiteren Labor, in dem gegebenenfalls die Probenaufarbeitung oder eine Aliquotierung in Unterproben erfolgt. Die Probe wird in der Probenbank eingelagert; entsprechende organisatorische Daten (OrgDAT, z.B. Probennummer, Probenaufenthalt, Probencharakterisierungen) werden dokumentiert. Ist die Probenbank an ein geeignet ausgestattetes Institut angeschlossen, so können in der Probenbank auch direkt Analysen der Probe vorgenommen werden. Je nach Organisationsform des Forschungsverbunds geschieht dies im Zuge der Behandlung des Patienten, für ein konkretes Forschungsprojekt oder allgemein für Forschungszwecke. Analysen können auch durch andere Einrichtungen durchgeführt werden, wozu die Probe entsprechend zugeliefert werden muss, in der Regel nur von einem minimalen Satz organisatorischer Daten begleitet.

Zweck des Biobankenmoduls ist die medizinische Forschung mit Proben, Analyseergebnissen und Annotationsdaten. Dazu tritt in der Regel ein Forschungsprojekt mit einer bestimmten Anforderung (Spezifikation der Erkrankung, Randparameter wie Alter und Komorbiditäten, genetische Parameter, Anforderungen an die Probe bzw. deren Analyse) an den Forschungsverbund heran und erhält im Gegenzug Daten, eventuell auch Proben, die gemäß den Richtlinien des Forschungsverbundes bereitgestellt werden.

Biomaterialien werden oft auch im Rahmen einer klinischen Studie gesammelt. Solange sie an die Zweckbestimmung der Studie gebunden bleiben und überschüssige Reste spätestens bei Beendigung der Studie vernichtet werden, gelten hierfür die Regeln der Studie, die allgemein im AMG und den GCP-Richtlinien, im Speziellen in der Einwilligungserklärung festgeschrieben sind (vgl. Kap. 5.2, Studienmodul). Die Proben können im Rahmen der Studie direkt den Daten zugeordnet werden, so dass keine weiteren Anforderungen an das Identitätsmanagement (Kap. 6.1) entstehen. Sollen Proben über das Studienende hinaus langfristig aufbewahrt werden, so sind sie spätestens dann in ein eigenständiges Biobankenmodul zu überführen und unterliegen von da an den in diesem Kapitel beschriebenen Regeln. All dies kann natürlich nur auf der Grundlage einer ausreichenden Einwilligung geschehen. Gleiches gilt, wenn die Proben zwar für die Studie erhoben, aber direkt in einer Biobank aufbewahrt werden sollen; die Studie kann für ihre Zwecke wie jedes andere Forschungsprojekt Analysen und Auswertungen anfordern (s. o.). Auch die aus der Studie entstandenen Annotationsdaten sind spätestens bei Studienende in eine geeignete Annotationsdatenbank zu überführen.

5.4.2 Anwendungsfälle

Da die relevanten Anwendungsfälle bereits in dem generischen Datenschutzkonzept für Biobanken aus dem Jahr 2006 [2] beschrieben wurden, wenn auch anders strukturiert als für die anderen hier beschriebenen Module, wird an dieser Stelle auf eine wiederholende Beschreibung verzichtet. Tabelle 1 bietet eine Übersicht über die relevanten Anwendungsfälle, die der Strukturierungsvorgabe für Anwendungsfälle aus diesem Leitfaden folgt. Zu jedem Anwendungsfall sind die Verweise zu den entsprechenden Kapiteln des bereits veröffentlichten Konzepts für Biobanken aufgeführt. Ergänzend sind Verweise zu relevanten analogen Anwendungsfällen oder übergreifenden Kapiteln aus diesem Konzept aufgeführt.

Tab. 1 Anwendungsfälle im Biobankenmodul

Anwendungsfall	Relevante Kapitel im generischen Datenschutzkonzept für Biobanken	Vergleichbare Kapitel in diesem Leitfaden
Probenspender in eine Biobank aufnehmen	Kap. 4.2.2: Gewinnung und Anmeldung einer Probe *siehe auch:* Kap. 4.4.5: Probenmanagement	Kap. 5.1.2.1 Kap. 5.2.2.1
Daten auswerten	Kap. 1.1.2: Kennzeichnungen und Datentypen Kap. 4.4.5: Probenmanagement	
Ergebnisse mitteilen	Kap. 3.4: Wissen/Nichtwissen, Mitteilungspflichten	Kap. 5.3.2.8
Auskunft geben	Kap. 4.4.6: Auskunft an den Probanden	Kap. 5.3.2.6
Daten an Forscher weitergeben	Kap. 4.2.3: Erzeugung und Verschlüsselung der LabID Kap. 4.4.4: Bereitstellung von Daten *siehe auch:* Kap. 4.1.1: Aufgabe des Datenschutzkonzepts Kap. 4.4.5: Probenmanagement Kap. 3.3.3: Einwilligungserklärung – Weitergabe an Dritte	
Machbarkeit einer Studie prüfen	*nicht behandelt*	Kap. 5.1.2.9 Kap. 5.3.2.4
Rekrutierung unterstützen	Kap. 4.4.3: Pseudonymisierungsdienst *(für den Aspekt der Depseudonymisierung)* Kap. 3.8: Zusatzerhebung *(für den Aspekt der erneuten Kontaktierung)*	Kap. 5.1.2.10 Kap. 5.3.2.5
Proben und Daten sperren, anonymisieren, löschen oder vernichten	Kap. 3.7: Widerruf und Löschung Kap. 4.2.7: Widerruf einer Einwilligung Kap. 4.2.6: Anonymisierung Kap. 3.3.2: Nutzungsdauer, Sterbefall *(für die Aspekte der Aufklärung und Einwilligung)*	Kap. 5.2.2.11 Kap. 5.1.2.8 Kap. 5.2.2.11

5.4.3 Daten und Datenflüsse

Personendaten oder identifizierende Stammdaten (IDAT), Pseudonyme (PID und PSN) sowie medizinische Daten (als Annotationsdaten) kommen im Biobankenmodul in der gleichen Bedeutung wie in den anderen Modulen vor (s. Kap. 4.2 zum allgemeinen Datenmanagement in [2]). Daneben gibt es auch noch die folgenden Biobank-spezifischen Daten:

Probennummer (LabID): LabID bezeichnet die ursprüngliche Nummer der Probe, die entweder von der Proben gewinnenden Stelle oder von der Probenbank vergeben wird, in der Regel auch als Barcode-Aufkleber (Details in Kap. 4.2 zum allgemeinen Datenmanagement in [2]). Die LabID wird entweder durch die Proben gewinnende Stelle oder durch das verarbeitende bzw. analysierende Labor an die Annotationsdatenbank (vom Typ KDB oder FDB) gemeldet. Dort wird evtl. statt der LabID eine kryptographisch transformierte $LabID_{tr}$ gespeichert, um eine direkte Zuordnung von Datensatz und Probe zu vermeiden (s. Kap. 4.2.3 zur Erzeugung und Verschlüsselung der LabID in [2]). Diese Transformation ist logisch eine Funktion des Identitätsmanagements; wo sie tatsächlich durchgeführt wird, hängt von den konkreten Gegebenheiten des Forschungsverbunds ab (s. Kap. 4.2.3 in [2] und Kap. 6.1.3.1 in diesem Leitfaden). Dabei spielen auch Überlegungen zur Verhältnismäßigkeit eine Rolle (s. Kap. 4.6 in [2] und Kap. 6.7 in diesem Leitfaden).

Organisatorische Daten (OrgDAT): OrgDAT sind Begleitdaten einer Probe, die an unterschiedlichen Stellen entstehen und verwendet werden. So erfasst z.B. die Proben gewinnende Stelle die Probenart und gegebenenfalls die Informationen zu Probenentnahme und Präanalytik. In der Probenbank werden die Begleitdaten einer Probe mit weiteren Informationen wie z.B. den Umständen von Konservierung, Lagerung und Qualität gespeichert. OrgDAT zu einer Probe werden an verschiedenen Stellen benötigt und dann zur Unterscheidung durch unterschiedliche Indizes gekennzeichnet. Eine ausführliche Darstellung findet sich in den Kapiteln 1.1.2 (Kennzeichnungen und Datentypen) und 4.2.4 (Grundsätzliche Verteilung der Daten) in [2] sowie in Kapitel 6.5.2.4 in diesem Leitfaden.

Probenanalysedaten (AnaDAT oder ProbDAT): Die mit AnaDAT bezeichneten Ergebnisse der Probenanalyse werden in einer Analysendatenbank gespeichert, die im Biobankenmodul angesiedelt ist. Sie werden nach Bedarf für Anfragen verwendet oder an anfragende Forscher übermittelt (s. Kap. 1.1.2 in [2]). Die ihnen zu Grunde liegenden Analysen können sowohl von den der Probenbank angeschlossenen Laboren als auch von kooperierenden Einrichtungen durchgeführt werden. AnaDAT können potenziell rückbeziehbare Größen darstellen wie z.B. im Fall von Genotypen. Ihre Speicherung sollte daher separat von den Annotationsdaten und eventuellen anderen Datenbeständen des Forschungsverbundes im Biobankenmodul selbst erfolgen.

Insgesamt sind im Grundmodell eines Biobankenmoduls zumindest die folgenden Datenarten unter getrennter Verantwortung zu speichern:

- IDAT,
- MDAT,
- Probe (+ zugehörige OrgDAT) und AnaDAT.

Für die Zuordnung dieser getrennten Teildatenbestände werden die Kennungen

- PID,
- PSN,
- LabID,
- $LabID_{tr}$

als Pseudonyme verwendet, die jeweils nur unter genau definierten Bedingungen miteinander verknüpfbar sind, siehe auch Kapitel 6.1 (Identitätsmanagement) und Abbildung 7.

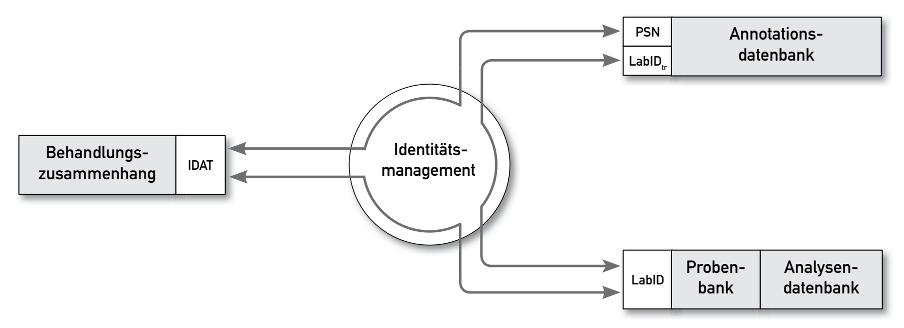


Abb. 7 In den Annotationsdaten einer Biobank sind die Verweise auf den Patienten und auf die zugehörigen Proben pseudonymisiert.

Für die Datenflüsse sei auf das Kapitel 4.2 zum allgemeinen Datenmanagement von [2] verwiesen.

5.4.4 Nutzer, Rollen und Rechte

Das Biobankenmodul betrachtet überwiegend die Rollen des Proben gewinnenden Arztes (dies können auch mehrere Ärzte für jeden einzelnen Spender sein) und des Wissenschaftlers, dazu verschiedene Systemadministratoren.

Probengewinnender Arzt: Übermittelt die Probe, ggf. über ein zwischengeschaltetes Labor, an die Probenbank und die Annotationsdaten an die Annotationsdatenbank. Weitere Zugriffe auf die Daten des Falls sind für den Proben gewinnenden Arzt im Rahmen des Biobankenmoduls nicht notwendig; ist das Biobankenmodul aber Teil eines Forschungsverbunds, der die Annotationsdaten in einer Klinischen, Studien- oder Forschungsdatenbank speichert, sind die dort (Kap. 5.1 bzw. 5.2 bzw. 5.3) vorgesehenen Zugriffsrechte zu gewähren.

Laborarzt: Analysiert eine Probe im Behandlungszusammenhang und übermittelt die Ergebnisse sowohl an die Analysendatenbank als auch an den Proben gewinnenden Arzt im Rahmen der Labordiagnostik des Behandlungsfalls oder der klinischen Studie.

Analysierender Wissenschaftler: Analysiert eine Probe außerhalb des Behandlungszusammenhangs für die Nutzung in der Biobank und übermittelt die Ergebnisse an die Analysendatenbank. Für den Patienten relevante Ergebnisse werden gemäß der Regularien der Biobank bzw. des Forschungsverbunds an den Proben gewinnenden Arzt übermittelt.

Auswertender Wissenschaftler: Tritt an die Biobank mit einem Projektvorschlag heran und erhält Daten, evtl. auch Proben, wie in Kapitel 5.4.1 beschrieben.

Systemverwalter: Wird für die Probensammlung, die OrgDAT-Datenbank, die Analysendatenbank, die Annotationsdatenbank wie in Kapitel 5.1.4.5 (Klinisches Modul – Administrator für eine Klinische Datenbank) bzw. Kapitel 5.3.4 (Forschungsdatenbank – Nutzer, Rollen und Rechte) und die Komponenten des Identitätsmanagements (wie in Kap. 6.1.4.1 und 6.1.4.2) benötigt. Er hat bei den jeweils anderen Datenbanken keinerlei Rechte.

Auditor: Überprüft den ordnungsgemäßen Ablauf aller Prozesse im Biobankenmodul. Ein Zugriff auf IDAT ist dazu nicht notwendig.

Doppelrolle Arzt/Forscher: siehe Kapitel 4.1.1 (Aufgabe des Datenschutzkonzepts – Doppelrolle Arzt/Forscher) von [2] und die analogen Ausführungen in Kapitel 5.3.4 (Forschungsdatenbank – Nutzer, Rollen und Rechte) und Kapitel 6.2.3.3 (Rechtemanagement – Mögliche Rollenkonflikte).

5.4.5 Verantwortlichkeiten

Die Verantwortlichkeiten im Biobankenmodul sind in den Kapiteln 4.3–4.5 (Realisierung – Organisation der Biomaterialbank, Dienste, Verträge und Regelungsbedarf) von [2] abgehandelt. Allgemeine Aussagen, die für alle Forschungsverbünde gelten, sind in Kapitel 6.6 (Organisatorische Regelungen) zusammengefasst.

5.4.6 Besondere Aspekte der Realisierung

Für verschiedene Organisationsmodelle eines Biobankenmoduls siehe die Kapitel 2.1 (Trägerschaft der Biomaterialbank) und 4.3 (Realisierung – Organisation der Biomaterialbank) von [2]; für Überlegungen zur Verhältnismäßigkeit siehe das dortige Kapitel 4.6 (Überlegungen zur Verhältnismäßigkeit) sowie Kapitel 6.7 (Kriterien der Verhältnismäßigkeit) unten.

Das Betreiben eines Biobankenmoduls erfordert besondere Erweiterungen der Aufklärung und Einwilligung; diese sind im Kapitel 3 von [2] zur Einwilligungserklärung beschrieben.

Im Zusammenhang mit klinischen Studien sind drei Szenarien zu unterscheiden, siehe Kapitel 5.4.1 oben:

1. Probenverwendung direkt und nur im Studienkontext: Hier sollte, soweit vorhanden, ein in die Studiensoftware integriertes Probenmanagement genutzt werden.
2. Probenverwaltung in einer auch unabhängig von der Studie existierenden Biobank: Hier ist die Studie als Forschungsprojekt zu betrachten, das die Dienste der Biobank nutzt.
3. Übergabe von überschüssigen Proben an eine Biobank nach Beendigung der Studie: Hier ist die Studie in der Rolle eines Probenzulieferers zu sehen.

In den Fällen 2 und 3 sind die Prozesse des Identitätsmanagements nach den Regeln der Biobank einzuhalten.

Die Handhabung von LabID und $LabID_{tr}$ ist im BMB-Konzept [2] auf spezielle Weise beschrieben; ist das Biobankenmodul in einen größeren Forschungsverbund eingegliedert, kann die Verwaltung dieser beiden Pseudonyme alternativ auch an geeigneten Stellen des zentralen ID-Managements angesiedelt sein.

Der Markt für Biobank-Software ist noch nicht konsolidiert; Biobank-Verwaltungsfunktionen sind z.T. auch in Labor-Software oder Studiensoftware integriert. Die TMF unterstützt mit ihren Arbeitsgruppen den Erfahrungsaustausch hierzu. Insbesondere in den Arbeitsgruppen IT-Infrastruktur und Qualitätsmanagement sowie Biomaterialbanken werden konkrete Fragen der Realisierung und nötiger Hardware- und Softwareausstattung umfangreich diskutiert. Den Kontakt zu den Arbeitsgruppen vermittelt die TMF-Geschäftsstelle.

6 Organisatorisches und technisches Konzept für Forschungsverbünde

Ein medizinischer Forschungsverbund umfasst in der Regel mehrere oder alle der in Kapitel 5 beschriebenen Module. Durch deren Zusammenwirken ergeben sich komplexe Datenflüsse und Kommunikationsbeziehungen, die erhebliche organisatorische und technische Maßnahmen erfordern, auch zur Wahrung eines angemessenen Datenschutzniveaus. Auf der technischen Seite sind zentrale Komponenten und Verfahren vorzusehen, die für

- das Identitätsmanagement von Patienten und Probanden (Kap. 6.1), welches auch ein Kontaktmanagement einschließt,
- das Rechte- und Rollenmanagement für Netzteilnehmer (Kap. 6.2) und
- die Qualitätssicherung von Daten (Kap. 6.8)

zuständig sind und mit sorgfältig geplanten Sicherheitsmaßnahmen und -richtlinien, oft sogar bei organisatorisch unabhängigen Stellen (Trusted Third Parties, Datentreuhänder) betrieben werden.

Das Zusammenspiel verschiedener Module wird exemplarisch für den kombinierten Einsatz von

- Klinischem Modul und Studienmodul (Kap. 6.3) sowie
- Studien- und Forschungsmodul (Kap. 6.4)

erläutert; der kombinierte Einsatz von Forschungs- und Biobankenmodul war schon Gegenstand des Datenschutzkonzepts für Biomaterialbanken. Das Zu-

sammenspiel aller Module wird im Kapitel 6.5 als Maximalmodell beschrieben. Hinzu kommen Überlegungen und Vorschläge zu

- organisatorischen Regelungen (Kap. 6.6) und
- der Verhältnismäßigkeit von Maßnahmen (Kap. 6.7).

6.1 ID-Management

Das Identitätsmanagement für Patienten (und andere Studienteilnehmer) in einem medizinischen Forschungsverbund dient dazu,

- Daten, die zum selben Individuum gehören, korrekt zuzuordnen
- und dabei die Identität dieses Individuums vor Unberechtigten zu verbergen.

Diese beiden Ziele stehen in einem gewissen Spannungsverhältnis, da die korrekte Zuordnung eine Erkennbarkeit voraussetzt. Um diesen Zielkonflikt bestmöglich aufzulösen, werden sie generisch im Modul Identitätsmanagement zusammengefasst und auf zwei funktionale Komponenten aufgeteilt, deren Zusammenspiel sorgfältig austariert werden muss. Diese beiden Komponenten werden hier als

- Patientenliste und
- Pseudonymisierungsdienst

bezeichnet. Sie werden in Kapitel 6.1.1 in ihren Funktionen und in Kapitel 6.1.5 in ihrer organisatorischen Ausgestaltung beschrieben. Wie weit diese konzeptionelle Aufteilung des Identitätsmanagements in zwei Komponenten bei einer Implementierung abgebildet werden muss oder kann, ist Gegenstand späterer Erläuterungen.

Die persönliche Identifikation eines Patienten soll nur den unmittelbar an seiner Behandlung Beteiligten möglich sein, nicht aber anderen, z.B. wissenschaftlich tätigen Mitarbeitern des Forschungsnetzes. Außerhalb des direkten Behandlungskontexts ist daher – da die Ziele eines medizinischen Forschungsverbundes in der Regel mit anonymisierten Daten nicht erreicht werden können – ein pseudonymes Identitätsmanagement aufzubauen. Sinngemäß gilt das gleiche für Studienteilnehmer (Probanden), die nicht Patienten sind (z.B. Kontrollpersonen, Teilnehmer an epidemiologischen Studien).

6.1.1 Zweck und Verwendungsbereich

Patienten oder Studienteilnehmer werden in verschiedenen Bereichen des Forschungsverbundes durch unterschiedliche pseudonyme Kennzeichen repräsentiert[26]:

26 Die unterschiedlich aufgebauten Bezeichnungen und Akronyme für die verschiedenen Pseudonyme resultieren aus dem historischen „Wildwuchs“ und den in anderen Kontexten bereits etablierten Nomenklaturen.

- PID_K: im Klinischen Modul
- PID_S: im Studienmodul
- SIC: im Studienmodul für einzelne Studien
- PSN: im Forschungsmodul
- LabID: zur Kennzeichnung von Proben im Laborbereich (Probenbank)
- $LabID_{tr}$: zur Kennzeichnung von Proben im Forschungsmodul

Siehe hierzu auch Abbildung 8. Eventuell kommen dazu weitere Pseudonyme wie PID_B in einer Bilddatenbank, sofern eine solche unter getrennter Datenhoheit geführt wird, temporäre Pseudonyme für die Verarbeitung im Grid oder in der Cloud (vgl. Kap. 6.1.3.7) oder PSN_I für Datenexporte an Forschungsprojekte.

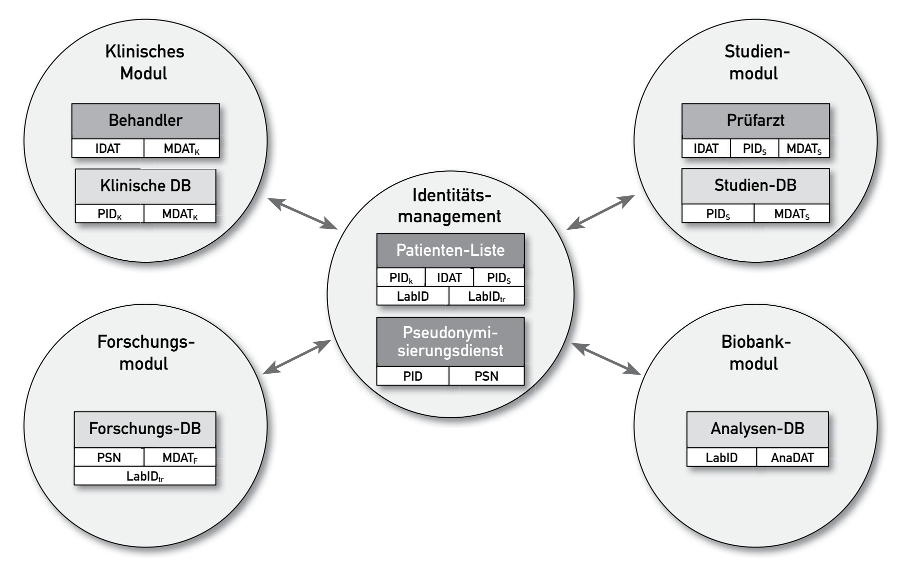


Abb. 8 Die zentrale Stellung des Identitätsmanagements; die Akronyme sind in Tabelle 2 zusammengestellt.

Grundsätzliche Aufgabe des Identitätsmanagements ist, die Zuordnung dieser Pseudonyme zueinander und zu den Identitätsdaten in den Anwendungsfällen, die dieses erfordern, herzustellen. Für solche Zuordnungs- oder Depseudonymisierungsprozesse sind nach den Regeln des Forschungsverbundes Entscheidungsprozesse und Kontrollen notwendig; das Identitätsmanagement soll organisatorisch und technisch so gestaltet werden, dass diese Regeln unterstützt bzw. erzwungen werden.

6.1.1.1 Patientenliste (mit PID-Dienst und IDAT-Datenbank)

Zweck der Patientenliste ist die Anmeldung und Registrierung eines Patienten oder Studienteilnehmers im Forschungsverbund sowie die Zuordnung eines eindeutigen nichtsprechenden Identifikators zu den Identitätsdaten IDAT.

Tab. 2 Akronyme

Abkürzung	Bedeutung	Verwendung
IDAT	Identitätsdaten	Direkter Behandlungszusammenhang
PID	(nichtsprechender) Patientenidentifikator	im Pseudonymisierungsdienst, im generischen Fall PID = PID_S, aber auch PID = PID_K möglich
PID_K	(nichtsprechender) Patientenidentifikator	Klinisches Modul
PID_S	(nichtsprechender) Patientenidentifikator	Studienmodul
SIC	(nichtsprechender) Subject Identification Code	einzelne Studie oder Studien-DB
PSN	Pseudonym	Forschungsmodul
LabID	Probenkennzeichnung	Biobank
$LabID_{tr}$	Verschlüsselte Probenkennzeichnung	Forschungsmodul
$MDAT_K$	Medizinische Daten	Klinisches Modul
$MDAT_S$	Medizinische Daten	Studienmodul
$MDAT_F$	Medizinische Daten	Forschungsmodul
AnaDAT	Analysedaten aus Proben, insbesondere genetische Daten	Biobank
OrgDAT	organisatorische Daten	siehe Kapitel 6.5.2.4

Dieser Identifikator wird hier zunächst als PID bezeichnet und kann als Pseudonym oder als Teil der IDAT behandelt werden. Es kann sich dabei um einen PID_K (aus dem Klinischen Modul) oder PID_S (aus dem Studienmodul) handeln, je nachdem, welche dieser beiden Kennungen in diesem Forschungsverbund benötigt wird oder aus welchem Bereich die Anmeldung erfolgt. Je nach Meldeweg wird diese Kennung

- an der Datenquelle erzeugt und an die Patientenliste übergeben
- oder erst dort erzeugt bzw. aus dem schon vorhandenen Bestand entnommen;

die andere der beiden (sowie weitere benötigte) Kennungen wird daraus in der Software der Patientenliste durch eine kryptographische Transformation abgeleitet. Werden im Verbund mehrere klinische Studien mit verschiedenen SICs durchgeführt, wird die Zuordnung zwischen diesen und dem PID_S ebenfalls in der Patientenliste zusammen mit dem Hinweis auf den Kontext der jeweiligen Kennung ($OrgDAT_{PL}$) aufbewahrt. Dieser Kontext enthält Angaben zur meldenden Stelle und das Meldedatum, um einen für den Patienten verantwortlichen Arzt als Ansprechpartner identifizieren (s.a. Kap. 6.5.2.4) und im Bedarfsfall einen Kontakt herstellen zu können.

Die eindeutige Identifikation des Patienten durch die Patientenliste wird als ein Mittel der Qualitätssicherung verstanden. Zugrunde liegt ein Szenario, in

dem ein Patient mit einer chronischen oder langwierigen Erkrankung über einen längeren Zeitraum von unterschiedlichen Einrichtungen behandelt oder beobachtet wird. Ein Patient kann also von verschiedenen Stellen zu unterschiedlichen Zeitpunkten zur Teilnahme am Forschungsverbund angemeldet oder seine dort bereits vorhandenen Daten ergänzt werden. Durch die Arbeitsweise der Patientenliste soll sichergestellt werden, dass ein einmal angemeldeter Patient bei einer späteren Meldung wieder erkannt wird. Die Identifikation eines Patienten geschieht über die Stammdaten (IDAT), welche den Patienten im Klartext identifizieren und in der Patientenliste gespeichert werden. Über die IDAT ist im Bestand dieser Liste zu prüfen, ob der Patient bereits erfasst und ein PID vergeben ist. Im negativen Fall ist ein neuer PID zu erzeugen und mit den IDAT in den Bestand der Patientenliste zu übernehmen. Eine mögliche technische Komponente zur Umsetzung einer solchen Patientenliste ist der PID-Generator der TMF.

Ein wichtiges Problem der Identifikation besteht darin, sicherzustellen, dass bei der Vergabe des PID Synonymfehler (ein Patient hat mehrere PIDs) und Homonymfehler (zwei oder mehr Patienten haben einen identischen PID) mit möglichst hoher Sicherheit vermieden werden, und zwar auch dann, wenn die IDAT durch Änderung (z.B. des Namens) oder durch unterschiedliche Schreibweise oder Eingabefehler voneinander abweichen. Dazu dienen folgende Maßnahmen:

Die Erhebung der IDAT wird möglichst einheitlich gestaltet. Als Basis der IDAT wird der Datensatz der Versichertenkarte (VK oder eGK) empfohlen, da hiermit das größtmögliche Maß an Normierung erreicht wird und durch elektronische Übernahme der Daten fehlerhafte Eingaben vermieden werden können. Nach dem Rechtsgutachten [11] sind nicht direkt versorgungsbezogene Daten, wie z.B. Angaben zur Versicherung und insbesondere der lebenslang konstante Teil der Versichertennummer, hierfür allerdings nicht nutzbar (s. Kap. 4.3.2).

Zusätzlich soll der Geburtsname oder ein anderer früherer Name erfasst werden, wenn ein Patient während seiner Verweilzeit im Forschungsnetz den Namen gewechselt hat.

Für den Bestandsabgleich wird ein fehlertoleranter Algorithmus mit einstellbarer Empfindlichkeit verwendet.

Unklare Zuordnungen können durch manuellen Eingriff eines Administrators und ein Rückfragemanagement aufgelöst werden.

Mit der Anmeldung eines Patienten oder Studienteilnehmers bei der Patientenliste werden ein Kennzeichen der meldenden Stelle und das Datum der Meldung übertragen und in der Liste gespeichert. Dies gilt auch dann, wenn einem Patienten bereits ein PID zugewiesen wurde und dieser einer neu meldenden Klinik übermittelt wird. Kennzeichen und Datum werden nicht als Historie geführt, sondern durch die jeweils aktuelle Meldung überschrieben.

Die Daten ($OrgDAT_{PL}$ mit Kontextinformation) werden benötigt, damit die Stelle, welche die Patientenliste führt, erkennen kann, über welche Klinik oder welchen verantwortlichen Arzt in einem entsprechenden Anwendungsfall ein Patient kontaktiert werden kann. Sie können auch als Entscheidungshilfe bei der Prüfung von Zugriffsberechtigungen herangezogen werden (s.a. Kap. 6.5.2.4).

Die Funktion der Patientenliste ist weitgehend automatisiert. Bei der Anmeldung eines Patienten können Fälle auftreten, in denen die Zuordnung der Meldung zum Bestand der Liste zwar möglich, aber wenig gesichert ist. Ein solcher Fall führt zu einer Fehlermeldung. Abhängig davon, wie wichtig es für die Forschungsziele ist, Synonyme und Homonyme zu vermeiden, kann für solche Fälle ein Verfahren zum manuellen Abgleich von Daten vereinbart werden; bei der Führung der Patientenliste ist dann der Eingriff durch einen Operator bzw. eine Dokumentationsfachkraft erforderlich.

Hinweis: Das Identitätsmanagement bei einzelnen Projekten, insbesondere klinischen Studien nach AMG, ist evtl. unabhängig zu betreiben, da eine Systemvalidierung bei zentral genutzten Diensten wesentlich erschwert ist; dies wird relevant, sobald das Identitätsmanagement mit Fehlerkorrektur- und Record-Linkage-Mechanismen versehen ist. Daher ist es hier in der Regel zu empfehlen, dass der Prüfarzt einen SIC vergibt oder einmalig aus einer externen Quelle übernimmt, der nur ihm – und darüber hinaus bei Notwendigkeit der Patientenliste im Verbund – bekannt ist. Ein solcher Mechanismus zur SIC-Erzeugung ist in der Regel in der Studiensoftware implementiert.

6.1.1.2 Pseudonymisierungsdienst

Zweck des Pseudonymisierungsdienstes ist der besondere Schutz der Daten in dem auf Langzeitspeicherung angelegten Forschungsmodul. Mittel dazu ist die Transformation des PID aus der Patientenliste in ein Pseudonym PSN, das in der Forschungsdatenbank als Kennung genutzt wird; hierfür wird ein kryptographisches Verfahren angewendet. Der Datenfluss in die Forschungsdatenbank wird über den Pseudonymisierungsdienst geleitet, wobei der PID durch das PSN ersetzt wird. Da der Pseudonymisierungsdienst die medizinischen Daten (MDAT) weder benötigt noch überhaupt sehen soll, werden diese in asymmetrisch verschlüsselter Form durchgereicht oder ganz an ihm vorbei geleitet, siehe Abbildung 9. Die zweite Option hat den Vorteil geringerer Anforderungen an die Bandbreite des Datendurchsatzes im Pseudonymisierungsdienst und den Nachteil erhöhter Komplexität der Kommunikation.

Die Pseudonymisierung ist eine reine Maschinenfunktion, die keines Eingriffs durch das Personal bedarf. Um eine unberechtigte Nutzung dieses Dienstes, der mit der Weiterleitung der Daten an die Forschungsdatenbank verbunden ist, auszuschließen, werden die Daten nur von zugelassenen Absendern übernommen (s. Kap. 6.1.4.2).

a) Nutzdaten (MDAT) werden verschlüsselt durchgereicht



b) Nutzdaten (MDAT) werden vermittelt



Abb. 9 Verschlüsselte Durchleitung oder Vorbeileitung von Daten; Aufgabe des Dienstleisters ist nur, pseudonyme Kennungen (z.B. PID und PSN oder LabID und $LabID_{tr}$) ineinander umzuwandeln.

Hinweis: Die Pseudonymisierung wird hier für die Patientendaten beschrieben. Sie kann in gleicher Weise eingesetzt werden, um die Kennung medizinischer Einrichtungen oder individueller Ärzte (ADAT) in den Forschungsdaten unkenntlich zu machen. Selbstverständlich ist dies auch in einem nachfolgenden Schritt beim Export von Daten aus der Forschungsdatenbank möglich. Die Lösung muss in der Vertragsgestaltung zwischen den Ärzten und dem Forschungsverbund und bei der Regelung des Zugangs zu Forschungsdaten definiert werden. Ein entsprechender Depseudonymisierungsvorgang muss eingerichtet werden.

6.1.2 Anwendungsfälle

a) **Anmeldung** eines Patienten oder Studienteilnehmers beim Forschungsverbund: Die direkte Anmeldung erfolgt bei der Patientenliste. Das Identitätsmanagement sorgt dafür, dass die nötigen pseudonymen Kennzeichen für die verschiedenen Bereiche des Forschungsverbundes erzeugt werden, siehe auch Abbildung 10.

b, c) **Übermittlung** von Daten an die Forschungsdatenbank aus dem Versorgungskontext (Fall b) oder aus dem Studienkontext (Fall c): Die für die Forschungsdatenbank asymmetrisch verschlüsselten Daten (MDAT) werden über das Identitätsmanagement geleitet, das die verwendete Kennzeichnung in das im Forschungskontext verwendete PSN umwandelt. Als Alternative können die MDAT auch mit Hilfe eines vom Pseudonymisierungsdienst vergebenen Zugriffstickets direkt an die Datenbank übergeben werden, siehe Abbildung 9.

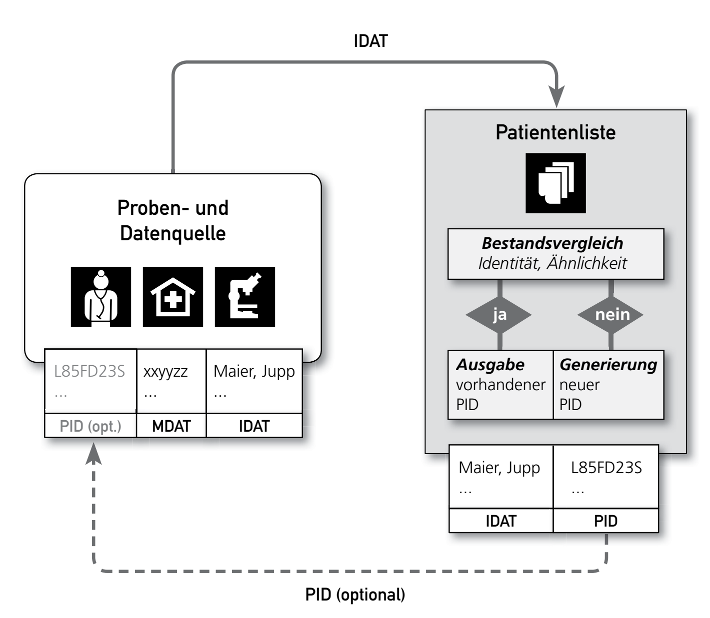


Abb. 10 Anmeldung eines Patienten oder Studienteilnehmers in der Patientenliste. Der pseudonyme Patientenidentifikator PID wird nur im Studienmodul (als PID_S), nicht aber im Klinischen Modul (als PID_K) zurückgemeldet.

d, e) **Mitteilung** von Ergebnissen (Findings) aus einem Forschungsprojekt (Fall d) an einen Patienten oder Studienteilnehmer: Hier wird über das Identitätsmanagement das Pseudonym in eine Kennung (in der Regel IDAT) umgewandelt, die dem für den Betroffenen verantwortlichen Arzt bekannt ist, und diesem das jeweilige Finding mitgeteilt; auch hier ist die asymmetrisch verschlüsselte Übertragung zu nutzen, siehe Abbildung 22 in Kapitel 6.8.3.2. Auf gleiche Weise kann auch auf **Anfragen** eines Patienten (Fall e) reagiert werden, sofern diese Art des Auskunftsrechts mit ihm vereinbart wurde. Hier wendet sich der Patient an seinen zuständigen Arzt oder einen sonstigen Auskunftsverpflichteten; dieser übermittelt die IDAT des Patienten über das Identitätsmanagement an die jeweilige Datenbank, die die Rückmeldung wie beschrieben veranlasst.

f) Die Depseudonymisierung zur **Datenqualitätssicherung** wird im Kapitel 6.8 über Qualitätssicherung behandelt.

g) Für die **Rekrutierung** von Studienteilnehmern für eine neue Studie – sofern dies aufgrund der Einwilligungserklärung erlaubt ist – wird der gleiche Weg zum verantwortlichen Arzt wie bei der Rückmeldung von Findings beschritten. Von diesem wird die Einwilligung des Betroffenen zur Teilnahme an dieser Studie eingeholt sowie dieser ggf. als Teilnehmer dieser Studie angemeldet.

h, i) Bei einem **Widerruf** der Teilnahme am Forschungsverbund werden, abhängig von der Vereinbarung in der Einwilligungserklärung, über das Identi-

tätsmanagement die entsprechenden Daten in den Datenbanken gefunden und **gelöscht** (Fall h) oder der Fall wird im Forschungsverbund **anonymisiert** (Fall i); das bedeutet hier einfach, dass in der Patientenliste – falls vorhanden, auch in dezentralen Patientenlisten – die IDAT gelöscht werden und somit der Bezug zum Individuum nicht mehr hergestellt werden kann. Im Einzelfall kann es hierbei auch nötig sein, charakteristische Merkmale der MDAT zu vergröbern oder zu löschen. Die Pseudonyme können, wenn mit Sicherheit niemand mehr darüber einen Personenbezug herstellen kann, als anonyme Kennzeichen in den jeweiligen Datenbanken verbleiben; ansonsten sind sie durch eindeutige anonyme Kennzeichen zu ersetzen.

j) Im **Todesfall** eines Patienten oder Probanden sind in der Regel, sobald eine Nachmeldung oder Nacherfassung von Daten nicht mehr zu erwarten ist, alle seine Daten im Forschungsverbund zu anonymisieren; die Regularien des Forschungsverbundes und die Einwilligungserklärung sind zu beachten. Da im Maximalmodell die Dauerspeicherung nur im Forschungsmodul vorgesehen ist, sind noch im Klinischen Modul oder Studienmodul befindliche Daten dorthin zu überführen und überall sonst zu löschen. Proben und Daten im Biobankenmodul können – sofern das vorgesehen und rechtlich abgesichert ist – ebenfalls erhalten bleiben, und ebenso muss die Assoziation zwischen Daten im Forschungsmodul und Biobankenmodul über PSN und LabID bzw. $LabID_{tr}$ erhalten bleiben. In der Patientenliste sind die IDAT und alle nicht mehr benötigten pseudonymen Kennungen zu löschen.

k) Eine **Umpseudonymisierung** (Ersetzen vorhandener Pseudonyme durch neue) kann nötig werden, wenn einzelne Pseudonyme als kompromittiert erkannt werden oder wenn das Pseudonymisierungsverfahren insgesamt als unzureichend oder nicht mehr dem Stand der Technik (s. Kap. 2.6 des Kryptographischen Gutachtens im Anhang[27]) entsprechend eingeschätzt wird (vgl. zugehörigen Anwendungsfall in Kap. 6.4.2.10). Beim Verfahren ist zu unterscheiden, ob die Pseudonyme durch eine Zuordnungsliste oder eine kryptographische Transformation erzeugt wurden. Im Fall einer Zuordnungsliste, die willkürliche Pseudonyme ohne Verwendung eines deterministischen Algorithmus vergibt, ist nur der Fall der Kompromittierung einiger oder aller Pseudonyme relevant. Diese müssen dann durch neu vergebene Pseudonyme ersetzt werden, die auch an die jeweiligen Datenbanken des Forschungsverbundes weitergegeben werden. Die Möglichkeit, dass durch die Kompromittierung bereits Daten an Unbefugte gelangt sind, erfordert Reaktionen auf der organisatorischen Ebene des Forschungsverbundes, die aber das Identitätsmanagement nicht weiter involvieren.

Falls die Pseudonyme durch eine kryptographische Transformation vergeben wurden, ist der bisherige Algorithmus durch einen neuen ausreichender Stär-

27 Anhänge zu diesem Dokument sind unter www.tmf-ev.de/datenschutz-leitfaden verfügbar.

ke zu ersetzen; alle bisher vergebenen Pseudonyme müssen durch die nach dem neuen Algorithmus erzeugten ersetzt werden, vgl. Kapitel 2.6 des Kryptographischen Gutachtens im Anhang.

l) Der **Export medizinischer Daten für die Weitergabe an Forscher** ist ein Anwendungsfall, der alle Datenbanken eines Forschungsverbunds betreffen kann. Dabei sind nach Möglichkeit anonymisierte Daten herauszugeben, so dass die Erzeugung anonymer Datensatz-IDs als Funktion des ID-Managements genutzt werden kann. Wenn die Nutzung der Daten mögliche Implikationen für die betroffenen Probanden hat und die Auswertung pseudonymer Daten durch die Wissenschaftler z.B. durch eine Einwilligung rechtlich abgesichert ist, müssen die vorhandenen pseudonymen Kennzeichen der jeweiligen Datenbank durch für diesen Export spezifische neue pseudonyme Kennzeichen ersetzt werden. Um die Auswertungsergebnisse ggf. später wieder einem Probanden zuordnen zu können, muss der für diesen Export eingesetzte Schlüssel für die Umpseudonymisierung gespeichert werden. Auch diese exportspezifische Pseudonymisieurng kann als Funktion des ID-Managements realisiert werden.

m) Das **Aktualisieren der Kontaktdaten** von Patienten oder Probanden kann logisch einem zentralen ID-Management zugeordnet werden (vgl. Kap. 3.2.3.2). Wichtig ist dies, wenn der Forschungsverbund langfristig und ggf. auch studienübergreifend den Kontakt zu den Patienten oder Probanden halten möchte, z.B. um diese für neue Projekte zu rekrutieren oder über neue Ergebnisse zu informieren. Die mit dieser Aufgabe betrauten Mitarbeiter sollten keinen Zugriff auf medizinische Daten haben und auch die für die Pflege der Kontaktdaten nicht nötigen Pseudonyme nicht einsehen können. Wichtig ist das Vorliegen notwendiger Informationen aus den Einwilligungserklärungen, da diese im Regelfall die Rechtsgrundlage für ein direktes Ansprechen der Patienten oder Probanden aus dem Forschungskontext heraus darstellen. Ggf. kann für diesen Aufgabenbereich auch eine spezialisierte CRM-Software zum Einsatz kommen.

6.1.3 Daten und Datenflüsse

6.1.3.1 Daten der Patientenliste

Die Patientenliste speichert und verwaltet IDAT, PID_K, PID_S und zugehörige SICs sowie andere gegebenenfalls in anderen Modulen des Forschungsverbunds benötigte Kennungen wie LabID oder das Pseudonym einer Bilddatenbank (PID_B), außerdem die Kontextdaten $OrgDAT_{PL}$ (einschließlich ADAT). Sie sieht, kennt und speichert nicht MDAT und PSN. Die Verwaltung der pseudonymisierten $LabID_{tr}$ ist logischer Teil des Identitätsmanagements. Sie kann, wie in Abbildung 8 dargestellt, bei der Patientenliste angesiedelt sein. Als Option besteht auch die im generischen Datenschutzkonzept für Biomaterialbanken [2] vorgesehene Möglichkeit, die Zuordnung zwischen LabID und $LabID_{tr}$ der Probenbank als Aufgabe zu übergeben.

Die Patientenliste *erhält* die Daten IDAT und $OrgDAT_{PL}$ (s. Kap. 6.1.3.3 unten), je nach Szenario empfängt sie auch dezentral erzeugte Identifikatoren, z.B. SICs. Sie *gibt* den PID_K an die Klinische Datenbank *zurück*, den PID_S an die Studiendatenbank und an die Datenquelle (hier: Prüfarzt), je nach Szenario auch den PID_K an die Datenquelle (hier: behandelnder Arzt). Je nach Szenario gibt die Patientenliste auch Einmal-Kennungen (als Zugriffstickets) an einen behandelnden Arzt und die Klinische Datenbank, die temporär zur richtigen Zuordnung von Kommunikationsprozessen benötigt werden.

Es wird empfohlen, in der Patientenliste als PID primär den PID_S zu erzeugen, und zwar in menschenlesbarer Form (8 Buchstaben und Ziffern). Der PID_K – ebenso wie weitere benötigte Kennzeichen – wird daraus durch kryptographische Verschlüsselung gewonnen und ist eine nur maschinenlesbare Bitkette; dies ist angemessen, da der PID_K nur in der Kommunikation von Patientenliste mit Klinischer Datenbank genutzt wird und sonst nirgends sichtbar sein soll.

6.1.3.2 Daten des Pseudonymisierungsdienstes

Der Pseudonymisierungsdienst speichert keine Daten außer dem geheimen kryptographischen Schlüssel, der die Zuordnung zwischen PID_S und PSN vermittelt. Er *erhält* einen PID (im generischen Fall den PID_S) und *gibt* das zugehörige PSN *weiter*. Bei einer Depseudonymisierung ist dies genau umgekehrt (s. Kap. 6.1.3.5 unten).

Der Schlüssel für die Transformation PID ↔ PSN ist unauslesbar auf einer Smartcard oder in einer vergleichbar sicheren Umgebung wie z.B. einem Hardware Security Module (HSM) zu speichern, damit er sicher als Geheimnis bewahrt werden kann. Die kryptographischen Funktionen müssen ebenfalls in der sicheren Umgebung, z.B. auf der Smartcard, ausgeführt werden, damit der Schlüssel diese nicht verlassen muss.

6.1.3.3 Datenflüsse der Patientenliste

Die Anmeldung eines Patienten oder Studienteilnehmers beim Forschungsverbund erfolgt bei der Patientenliste. Mit dem dort erzeugten oder schon vorhandenen PID können dann medizinische Daten (MDAT) an die entsprechende Datenbank zusammen mit dem entsprechenden pseudonymen Kennzeichen übermittelt werden. Wird der PID nicht an die Datenquelle zurückgemeldet, wie es in einigen Szenarien sinnvoll ist, wird für die Datenübermittlung statt dessen ein von der Patientenliste erzeugtes Zugriffsticket (zum einmaligen Gebrauch) verwendet.

Auch bei der Depseudonymisierung wirkt die Patientenliste mit (s. Kap. 6.1.3.5 unten).

6.1.3.4 Datenflüsse des Pseudonymisierungsdienstes

Der Pseudonymisierungsdienst erhält einen PID_S von der Patientenliste und gibt das zugehörige PSN an die Forschungsdatenbank weiter (s. Abb. 11). Dazu werden die MDAT (aus dem Klinischen Modul oder Studienmodul) an die Forschungsdatenbank (FDB) nach einer von zwei Methoden übertragen (s. Abb. 9):

- asymmetrisch verschlüsselt über den Pseudonymisierungsdienst weitergeleitet oder
- mit Hilfe eines temporären Zugriffstickets, das die richtige Zuordnung garantiert, direkt von der Datenquelle.

Beiden Optionen ist gemeinsam, dass der Pseudonymisierungsdienst keine Möglichkeit hat, die MDAT zu lesen.

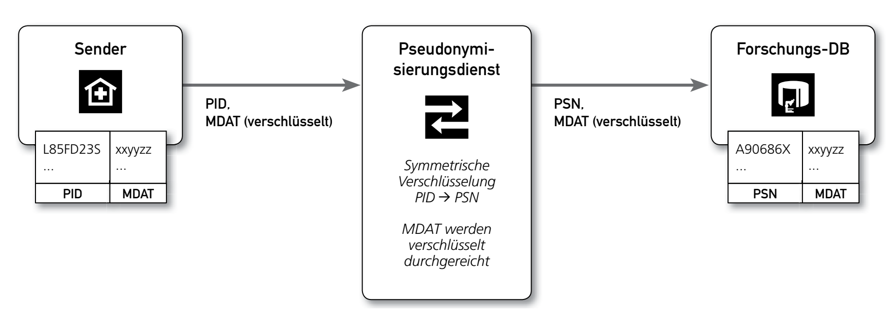


Abb. 11 Workflow des Pseudonymisierungsdienstes; alternativ ist auch eine getrennte Übermittlung der MDAT mit Hilfe eines Zugriffstickets möglich (s. Abb. 9).

In der Forschungsdatenbank werden die MDAT entschlüsselt und mit dem Pseudonym PSN abgespeichert. Der Vorgang ist aus der Sicht des Pseudonymisierungsdienstes unabhängig davon, ob die Daten neu geliefert werden oder ob eine Änderungsmeldung bereits in die Datenbank übernommene Daten korrigiert oder ergänzt. Nur der Betreiber der Datenbank muss und kann die beiden Formen unterscheiden.

Der Rückbezug von Daten aus der Forschungsdatenbank oder daraus abgeleiteten Auswertungen auf den betroffenen Patienten kann daher ausschließlich über den Weg der Depseudonymisierung, d.h. der kryptographischen Rücktransformation des PSN in den PID gewonnen werden (s. Kap. 6.1.3.5 unten).

Hinweis: Ein weiterer Pseudonymisierungsschritt wird für den Export der Daten empfohlen, wenn verhindert werden soll, dass außerhalb der zentralen Datenbank Akkumulationen von Daten erfolgen. Dabei wird das PSN jeweils durch eine weitere kryptographische Transformation oder eine willkürliche Zuordnungsliste in ein projektspezifisches PSN_I umgewandelt, das als Ordnungskriterium für Datenbestände gilt, die an das Forschungsprojekt Nr. *i* exportiert werden. Diese Transformation kann durch einen zentralen Pseudonymisie-

rungsdienst unterstützt werden, der sich auch die projektspezifische Zuordnungsliste oder den verwendeten Schlüssel für mögliche Rückmeldungen merkt. Alternativ kann dies auch im Rahmen der Exportfunktion einer Forschungsdatenbank realisiert werden.

6.1.3.5 Depseudonymisierung

Die Depseudonymisierung kann nur von einer berechtigten Einrichtung bzw. von berechtigten Personen nach dem Regelwerk des Forschungsverbundes veranlasst und nur vom Identitätsmanagement durchgeführt werden.

Technisch ist die Depseudonymisierung im generischen Fall zweistufig angelegt: Die erste Stufe wird auf dem inversen Weg der Pseudonymisierung durch die Transformation eines Pseudonyms PSN in einen Patientenidentifikator PID geleistet. Dazu erhält der Pseudonymisierungsdienst ein PSN, leitet daraus den zugehörigen PID ab und gibt diesen (zusammen mit organisatorischen Daten des Vorgangs) an die Patientenliste weiter; dieser Schritt kann in definierten Anwendungsfällen auch automatisiert ablaufen. In der zweiten Stufe wird der PID in der Patientenliste aufgrund einer Datenbank-Abfrage durch die Identifikationsdaten IDAT ersetzt. Diese werden zusammen mit den organisatorischen Daten des Vorgangs an den in den $OrgDAT_{PL}$ (bzw. ADAT) genannten Verantwortlichen weitergeleitet (s. Abb. 12).

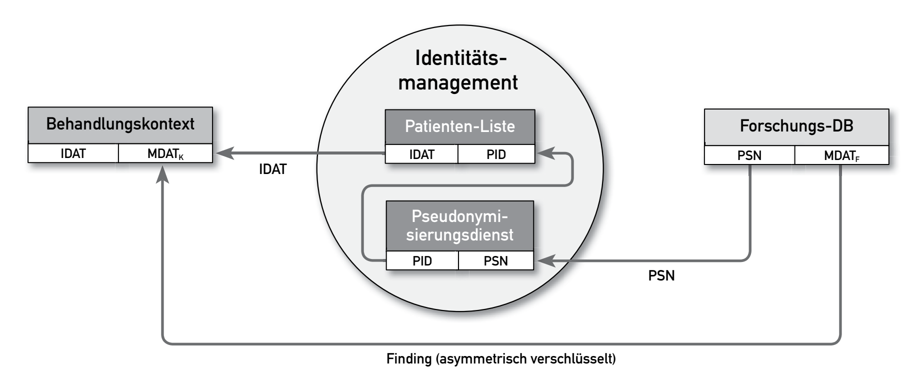


Abb. 12 Workflow der Depseudonymisierung im Anwendungsfall Rückmeldung (PID = PID_S oder PID_K je nach Kontext)

6.1.3.6 Umpseudonymisierung

Die Umpseudonymisierung im Falle einer Zuordnungsliste betrifft die Patientenliste mit dem primär erzeugten PID (im Regelfall PID_S) und erfordert folgenden Ablauf: Jeder zu ändernde PID wird vom Administrator der Patientenliste durch einen entsprechenden neuen ersetzt. Alle daraus erzeugten weiteren Kennungen in Patientenliste und Pseudonymisierungsdienst sind entsprechend

zu ändern und – zusammen mit der alten, zu ändernden Kennung – an die jeweiligen nutzenden Datenbanken zu übermitteln.

Im Falle einer kryptographischen Transformation ist zu unterscheiden, ob nur für einen Einzelfall eine Umpseudonymisierung nötig ist, oder ob wegen Kompromittierung des kryptographischen Verfahrens sämtliche Pseudonyme ausgetauscht werden müssen. Im ersten Fall wird ein neu erzeugter PID zusammen mit dem alten angeliefert und in ein neues PSN umgewandelt, das zusammen mit dem alten an alle relevanten Stellen im Forschungsmodul übermittelt und mit einer Änderungsaufforderung versehen wird.

6.1.3.7 Temporäre Pseudonyme in verteilten Infrastrukturen

Um umfangreiche medizinische Datensätze, wie sie z.B. die Bildgebung oder genetische Sequenzierungsmethoden produzieren, in vertretbarer Zeit und mit ökonomisch vertretbaren Mitteln verarbeiten und auswerten zu können, werden zunehmend verteilte Infrastrukturen, entweder als Grid oder Cloud, eingesetzt. Wenn diese Infrastrukturen nur für die Analyse der Daten und nicht für eine dauerhafte Speicherung eingesetzt werden, was insbesondere bei rechenintensiven Verarbeitungsschritten der Regelfall ist, kann der Schutzbedarf der Daten durch die Verwendung temporärer Pseudonyme noch weiter abgesenkt werden.

Hierfür werden zentral vom ID-Management netzweit eindeutige Pseudonyme bereit gestellt, die für einen Transfer eines Datensatzes in das Grid oder in die Cloud, die dortige Verarbeitung und die Rückübermittlung des Ergebnisses gültig sind. Diese werden ohne Übermittlung identifizierender Daten abgerufen und direkt nach Erhalt der Ergebnisse im ID-Management wieder freigegeben. Lediglich die Daten liefernde Stelle speichert während der Verarbeitung der Daten den Zusammenhang von temporärem Pseudonym und der Identität des zugehörigen Probanden oder Patienten. Im ID-Management wird das herausgegebene Pseudonym bis zur Freigabe durch die abrufende Stelle gesperrt und damit in dieser Zeit nicht erneut herausgegeben.

Bei komplexen Datenstrukturen, wie sie z.B. auch im DICOM-Header von Bildern und Bildserien vorkommen, müssen ggf. multiple Identifikatoren, wie beispielsweise global eindeutige IDs für jedes Bild, das bildgebende Gerät usw. ersetzt werden. In solchen Fällen müssen entweder mehrere temporäre Pseudonyme verwendet werden oder von einem temporären Pseudonym werden weitere abgeleitet, z.B. durch Suffixe oder Präfixe. Dabei ist aber auch zu berücksichtigen, dass für standardisierte Datenformate wie DICOM bestimmte Vorgaben bezüglich der verwendeten IDs eingehalten werden müssen.

Eine weitere Absenkung des Schutzbedarfs kann durch den zusätzlichen Einsatz eines Pseudonymisierungsdienstes erreicht werden, der die temporären Pseudonyme beim Transfer der Daten in das Grid oder in die Cloud durch symmetrisch verschlüsselte temporäre Pseudonyme zweiter Ordnung ersetzt

(s. Kap. 6.1.3.4). Bei der Rückübermittlung der Ergebnisse wird die Umschlüsselung im Pseudonymisierungsdienst wieder rückgängig gemacht, so dass an der Datenquelle die Ergebnisse wieder dem richtigen Patienten oder Probanden zugeordnet werden können. Bei komplexen Datenstrukturen mit multiplen, durch temporäre Pseudonyme ersetzten Identifikatoren müssen alle diese Kennungen beim Verschlüsseln berücksichtigt werden. Da in solchen Anwendungsfällen im Regelfall von größeren Datenmengen auszugehen ist, wird als Implementierungsvariante des Pseudonymisierungsdienstes diejenige empfohlen, bei der die Nutzdaten nicht asymmetrisch verschlüsselt durchgereicht, sondern vollständig an dem Pseudonymisierungsdienst vorbei geleitet und über Tickets korrekt zugeordnet werden (vgl. Kap. 6.1.1.2 und Abb. 9).

Zusätzlich zu den hier beschriebenen speziellen Verfahren im ID-Management sind in solchen Einsatzszenarien auch ergänzende organisatorische Regelungen zu treffen, die u.a. auch ein ausreichendes Schutzniveau im Grid oder in der Cloud garantieren. Weitere Hinweise dazu finden sich in Kapitel 6.6 und in den Ergebnisdokumenten der Projekte PneumoGrid und cloud4health[28]. Die TMF war bzw. ist in beiden Projekten an der Ausarbeitung datenschutzkonformer Umsetzungskonzepte beteiligt.

6.1.3.8 Todesfall

Abhängig davon, wo der Todesfall bekannt wird – in der Regel zuerst im Klinischen Modul, unter Umständen aber auch im Forschungsmodul, wenn dort Nacherhebungen oder Abgleiche mit Melderegistern oder epidemiologischen Registern vorgesehen sind, wird eine Meldung an das Identitätsmanagement gemacht, das die in Kapitel 6.1.2 j) vorgesehenen Löschungen veranlasst und entsprechende Rückmeldungen empfängt.

6.1.4 Nutzer, Rollen und Rechte

6.1.4.1 Patientenliste

Für die Patientenliste gibt es im Allgemeinen Nutzer aus meldenden Einrichtungen, die entweder über ein Web-Formular oder aus einem EDC-System heraus einen Patienten oder Studienteilnehmer melden können; zwischen Neumeldung und Nachmeldung mit geänderten IDAT wird dabei nicht unterschieden. Wird die Patientenliste nur im Batchbetrieb genutzt, gibt es diese externen Nutzer nicht; sie werden durch Sender bzw. Empfänger entsprechender Dateien ersetzt.

Die Patientenliste hat einen Systemadministrator. Dieser hat neben der rein technischen Server-Administration die Aufgaben

28 s. www.pneumogrid.de und www.cloud4health.de

- manuelle Korrektur von Datensätzen bei (z.B. telefonisch) gemeldeten Fehleingaben,
- manuelle Korrektur von Datensätzen bei Zweifelsfällen, in denen die Zuordnung nicht automatisch entschieden werden kann,
- gegebenenfalls Bedienung des Batchbetriebs

zu erfüllen und muss demnach die entsprechenden Rechte zugeteilt bekommen.

Der Eingriff eines Administrators ist auch dann erforderlich, wenn im Rahmen der Depseudonymisierung einem PID die IDAT zugeordnet werden sollen: Hier ist zuerst die Genehmigung zu prüfen; bei positivem Ergebnis muss der Zuordnungsvorgang manuell gestartet werden.

Der Administrator kann bei seinen Aufgaben von einer Dokumentationsfachkraft unterstützt werden; diese benötigt lediglich die Rechte zur manuellen Korrektur von Datensätzen.

6.1.4.2 Pseudonymisierungsdienst

Zur Nutzung des Pseudonymisierungsdienstes siehe Kapitel 6.1.1.2. Er wird bei beabsichtigter Übertragung von Daten an die Forschungsdatenbank durch die entsprechenden Kommunikationskomponenten einer Klinischen oder Studiendatenbank angestoßen, siehe Kapitel 6.1.6.2. Diese müssen die entsprechenden Rechte besitzen, siehe Kapitel 6.2. Direkte Nutzer gibt es für den Pseudonymisierungsdienst nicht; er kann nur als Netzdienst über die definierten Schnittstellen angesprochen werden.

Der Pseudonymisierungsdienst hat einen Systemadministrator mit den üblichen Aufgaben und Rechten. Dieser ist auch für das Anstoßen von Depseudonymisierungsvorgängen nach persönlicher Prüfung der Berechtigung des Vorgangs zuständig, sofern im Regelwerk des Forschungsverbunds für den konkreten Fall nicht ein automatisierter Prozess vorgesehen ist, ebenso für das Anstoßen von Umpseudonymisierungsvorgängen. Dem Systemadministrator obliegt auch die sachgemäße technische Handhabung der Smartcard bzw. des Hardware Security Modules, das den Pseudonymisierungsschlüssel enthält.

6.1.5 Verantwortlichkeiten

Die Gesamtverantwortung für das Identitätsmanagement liegt bei der Leitung des Forschungsverbundes und dem Ausschuss Datenschutz einschließlich dem Datenschutzbeauftragten. Dieser Personenkreis gibt insbesondere Richtlinien und Policies vor. Im Folgenden wird die organisatorische und technische Verantwortung für die Komponenten des Identitätsmanagements im Rahmen dieser Richtlinien beschrieben.

Im generischen Fall wird empfohlen, sowohl die Patientenliste als auch den Pseudonymisierungsdienst zentral für einen Forschungsverbund einzurichten, da so ein hoher Sicherheitsstandard erreicht werden kann und die erforderliche Infrastruktur und das zugehörige Personal nur einmal für den gesamten Forschungsverbund eingerichtet werden muss. Beide Dienste sollten bei unabhängigen vertrauenswürdigen Stellen (Trusted Third Parties, TTP) angesiedelt sein. Wenn diese Dienste separat an unabhängigen Stellen betrieben werden, ist eine zusätzliche wirksame Trennung zwischen den patientennahen Bereichen der Versorgung und der klinischen Forschung und dem patientenfernen Bereich der Forschungsdatenbank gegeben. Varianten dieser generischen Empfehlung werden in den folgenden Kapiteln diskutiert.

6.1.5.1 Patientenliste zentral oder dezentral?

Die Patientenliste kann an drei Stellen angesiedelt sein:

- zentral bei einer eigenen TTP,
- zentral zusammen mit dem Pseudonymisierungsdienst,
- dezentral an den Datenquellen.

Mit der zentralen Einrichtung der Patientenliste wird angestrebt, dass die Kranken- und Behandlungsgeschichten von Patienten mit einer chronischen oder rezidivierenden Erkrankung möglichst langfristig verfolgt werden können. Der Wechsel von Behandlungseinrichtungen und die räumliche Mobilität der Patienten führen dazu, dass Patienten im Lauf der Zeit von verschiedenen Einrichtungen an den Forschungsverbund gemeldet werden. Dann soll auch bei modifizierter Eingabe der IDAT (z.B. durch Schreibfehler bei manueller Erfassung oder Namensänderung) sichergestellt werden, dass der Patient oder Studienteilnehmer im Bestand identifiziert und ihm der bereits vorhandene PID zugewiesen wird.

Es ist zwar möglich, auch dezentrale Patientenlisten so anzulegen, dass mit einem für alle identischen Algorithmus aus identischen Eingabedaten ein identischer PID erzeugt wird, jedoch ist nicht zu vermeiden, dass modifizierte Eingabedaten zu einem neuen PID führen, so dass Synonyme entstehen. Die dezentrale Führung der Patientenliste hat außerdem den Effekt, dass auch die Depseudonymisierung nur dezentral, über die Stellen, die den Patienten persönlich kennen, möglich ist. Eine dezentrale Anordnung ist deshalb nur sinnvoll, wenn die Datenerfassung einmalig ist, wenn mit einem Wechsel des Patienten nicht gerechnet werden muss oder wenn eine Doppelerfassung unerheblich ist. Andererseits fördert die dezentrale Führung von Patientenlisten an den Datenquellen – d.h., bei der Erfassung der Identitätsdaten wird von einer behandelnden Einrichtung auch gleich ein nichtsprechender PID vergeben – in den genannten Fällen die Datensparsamkeit und ist somit vom Datenschutzgesichtspunkt aus unkritisch, zumal dieser Bereich von der ärztlichen Schweigepflicht abgedeckt und damit als vertrauenswürdig anzusehen

ist. In diesem Fall entfällt die Speicherung der ADAT in der Patientenliste, stattdessen kann die Speicherung der ADAT als Teil der MDAT angebracht sein; je nach Reidentifizierungsrisiko und Verhältnismäßigkeit ist auch von der elektronischen Speicherung der ADAT ganz abzusehen und nur eine Papierliste an geeigneter Stelle aufzubewahren.

6.1.5.2 Mehrere Patientenlisten an einem Standort?

Das Hosting mehrerer Patientenlisten von verschiedenen Netzen an einem Standort ist grundsätzlich möglich. Dabei müssen alle Prozesse und Verantwortlichkeiten geklärt und dokumentiert sein – z.B. durch entsprechende SOPs. Zur Umsetzung der notwendigen Mandantenfähigkeit finden sich hilfreiche Hinweise in der entsprechenden Orientierungshilfe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder [37]. Nicht geeignet ist allerdings das Hosting sämtlicher oder sehr vieler Patientenlisten bei einem einzigen Dienstleister, weil hier ein zu großes zentrales Angriffspotenzial entstünde.

Ebenfalls nicht geeignet ist das Konzept einer netzübergreifenden Liste für mehrere verschiedene Forschungsverbünde. Diese könnte zwar die Zugehörigkeit eines bestimmten Patienten zu einem bestimmten Forschungsverbund – und damit seine Diagnose – verschleiern. Da aber die Netzzugehörigkeit eines Patienten auch in einer netzübergreifenden Liste in irgendeiner Form vermerkt werden müsste, da sonst nicht überprüft werden kann, ob eine Anfrage nach den IDAT eines Patienten aus einem konkreten Netz heraus berechtigt ist oder nicht, wäre der Vorteil der Verschleierung auch in einer übergreifenden Liste nicht umsetzbar. Hierfür ist auch unerheblich, ob eine solche Anfrage schon im Ausschuss Datenschutz eines Netzes geprüft worden ist.

6.1.5.3 Sicherheit der Patientenliste

Die Patientenliste ist der sensibelste Teil des Identitäts-Managements und hat damit, wenn sie zentral geführt wird, eine besonders schützenswerte Rolle. Datenschutzrechtlich ist zu berücksichtigen, dass die IDAT, obwohl sie in der Patientenliste nicht mit medizinischen Daten (MDAT) kombiniert werden, den betroffenen Personenkreis als Patienten eines Forschungsnetzes mit einem umschriebenen Krankheitsspektrum ausweisen. Die Patientenliste ist daher unbedingt räumlich und technisch getrennt von den Datenbanken des Forschungsverbundes anzuordnen und auch einer getrennten disziplinarischen Verantwortung zu unterwerfen. Es muss ein praktikables und tragfähiges Sicherheitskonzept vorliegen, das sicherstellt, dass die Unabhängigkeit gewährt ist. Es empfiehlt sich, einer Partnereinrichtung des Forschungsnetzes diese zentrale Aufgabe zu übertragen, während die Datenbanken (KDB, SDB, FDB) bei anderen Partnern angesiedelt werden. Abweichend davon und bei besonders hohen Sicherheitsanforderungen besteht auch die Option, einen externen Datentreuhänder als TTP mit der Betreuung der Patientenliste zu beauftragen.

Hinweis: Der von der TMF bereitgestellte PID-Generator als Software-Implementierung der Patientenliste ermöglicht auch, die IDAT in einweg-verschlüsselter Form statt im Klartext abzulegen. Dies bewirkt einen zusätzlichen Schutz gegen das Reidentifizierungsrisiko, beeinträchtigt aber die manuelle Zuordnung in Zweifelsfällen und verhindert Anwendungen, bei denen eine Kontaktierung des Patienten erforderlich ist. Daher wird die Nutzung dieser Produkteigenschaft im Allgemeinen nicht empfohlen.

6.1.5.4 Lokalisierung des Pseudonymisierungsdienstes

Bei großen Forschungsverbünden – sobald für mehr als ein zeitlich beschränktes Forschungsprojekt pseudonymisiert werden muss – soll der Pseudonymisierungsdienst als zentraler Dienst selbstständig geführt werden. Zur Nutzung durch kleinere Verbünde wird empfohlen, den Pseudonymisierungsdienst als Dienstleistung von dritter neutraler Seite anzubieten, z.B. von der TMF selbst. Damit lässt sich verteilte Verantwortung kostengünstiger organisieren, als wenn jeder Forschungsverbund den Dienst selbst in einem eigenen Organisationsmodul realisiert.

6.1.6 Aspekte der Realisierung

6.1.6.1 Patientenliste

Die Patientenliste umfasst eine Funktion zur Erzeugung und Verwaltung der notwendigen Pseudonyme sowie zur Speicherung der zugehörigen Identitätsdaten (IDAT). Sie soll auf einem dedizierten Rechner geführt und in einem lokalen Netz geschützt aufgestellt werden. Die Kommunikation mit der Außenwelt erfolgt über einen kontrollierten Kanal (per Firewall-Tunnel) unter Nutzung des SSL-Protokolls oder gleichwertiger Lösungen.

Die TMF stellt als eine mögliche Komponente zur Umsetzung einer Patientenliste den PID-Generator zur Verfügung. Dieser kann

- online interaktiv über ein Web-Formular,
- offline im Batchbetrieb mit Datei-Übermittlung oder
- online als Web-Dienst aus einer externen Applikation (RDE-System) heraus

genutzt werden. Für letztere Nutzungsart ermöglicht die SOAP-Schnittstelle des PID-Generators in der jetzigen Implementierung die Client-Server- bzw. Server-Server-Kommunikation zwischen einer externen Applikation und der Patientenliste. Diese wird durch einen Webservice (SubjectList) realisiert und bietet Methoden zur Bearbeitung einer PID-Anforderung (Methode getSubjectID), zur Abfrage von Patientendaten (Methode getSubjectData) und zur Überprüfung der Gültigkeit eines PID (Methode isSubjectIDValid). Die Methode getSubjectID ruft den PID-Generator über die vorhandene CGI-Schnittstelle auf. Die Abfrage der Patientendaten bzw. der Validität eines PID wird direkt über eine SQL-Abfrage der Patientenliste durchgeführt.

Die folgenden Anforderungen, die mehrheitlich aus der hier neu vorgelegten Konzeption resultieren, sind in der bisher verfügbaren Version des PID-Generators noch nicht umgesetzt:

- Erzeugung und Verwaltung mehrerer zusammengehöriger pseudonymer Kennungen einschließlich deren Umwandlung,
- Entgegennahme und Verwaltung auch extern erzeugter Kennungen (z.B. SIC),
- Ausgabe geeigneter Zugriffstickets für die Kommunikation mit KDB, SDB und Pseudonymisierungsdienst,
- Überarbeitung und Erweiterung der Schnittstellen zur Kommunikation mit RDE-Software („SOAP-Schnittstelle“), KDB und SDB bzw. den dort angesiedelten Systemkomponenten des Pseudonymisierungsdienstes (s.u. in Kap. 6.1.6.2).

Die TMF wird zeitnah über mögliche Nachfolgeprodukte des PID-Generators informieren[29].

6.1.6.2 Pseudonymisierungsdienst

Die TMF hat eine Software zur Umsetzung eines Pseudonymisierungsdienstes[30] implementieren lassen, die von den folgenden Voraussetzungen ausgeht:

- Die Daten in Klinischen und Studiendatenbanken sind einfach pseudonymisiert mit einem eindeutigen PID_K oder PID_S.
- Der jeweilige PID ist für ein und dieselbe Person immer gleich, auch wenn diese Person in verschiedenen Einrichtungen behandelt wird oder an unterschiedlichen Studien zu unterschiedlichen Zeiten teilnimmt.
- Die Forschungsdatenbank kann das Attribut PSN speichern.

Über den Pseudonymisierungsdienst werden strukturierte Daten zwischen der Studien- (SDB) und der Forschungsdatenbank (FDB) ausgetauscht. Dazu müssen auf Seiten der SDB und der FDB Schnittstellen eingerichtet werden, um den Pseudonymisierungsdienst aufrufen und Daten in geeigneten Formaten übertragen zu können. Für diese Übertragungen gelten folgende Anforderungen:

Sie müssen je nach Richtung des Informationsaustausches einen PID_S (bei Nachrichten von der SDB an die FDB) oder ein PSN (bei Nachrichten von der FDB an die SDB) enthalten.

Die Nachricht kann über eine definierte Kennung (OrgDAT zum Vorgang) beschrieben werden, die Auskunft darüber erteilt, welche Reaktion von der

29 siehe http://www.tmf-ev.de/datenschutz-leitfaden

30 Im folgenden Textabschnitt wird die Bezeichnung Pseudonymisierungsdienst für das konkrete Softwareprodukt der TMF und nicht das davon unabhängige theoretische Konzept eines Pseudonymisierungsdienstes verwendet. Da sich sowohl für das Konzept als auch das Produkt mittlerweile die Bezeichnung Pseudonymisierungsdienst durchgesetzt hat, werden hier keine neuen separaten Namen eingeführt.

Gegenseite angefordert wird. Solche Reaktionen können sein: „Kontextdaten zu einem PID für die Qualitätssicherung senden", „Datensatz in FDB abspeichern", „Patient ein Finding anbieten" u.a.

Weiterhin kann die Nachricht medizinische Daten (MDAT) enthalten. Der Pseudonymisierungsdienst geht davon aus, dass diese Daten bereits auf Seiten der jeweils sendenden Datenbank verschlüsselt werden und insofern unabhängig davon, ob die Übertragungswege zum Pseudonymisierungsdienst ebenfalls SSL-gesichert sind, niemals im Klartext außerhalb der beiden Datenbanken sichtbar sind. Innerhalb der MDAT dürfen niemals personenidentifizierende Angaben (Namen, PID, PSN, Versicherungsnummern o.ä.) enthalten sein, da die MDAT vom Pseudonymisierungsdienst nicht verändert, sondern lediglich in verschlüsselter Form weitergeleitet werden.

Um diese Voraussetzungen zu gewährleisten, sind auf Seiten der Datenbanken spezielle Komponenten erforderlich, um die Kommunikation mit dem Pseudonymisierungsdienst zu ermöglichen. Diese, als SDB- bzw. FDB-Komponente bezeichnet, sind Teil der Software des Pseudonymisierungsdienstes, werden aber nicht dort, sondern bei der jeweiligen Datenbank implementiert. Abbildung 13 zeigt die Architektur des Pseudonymisierungsdienstes.

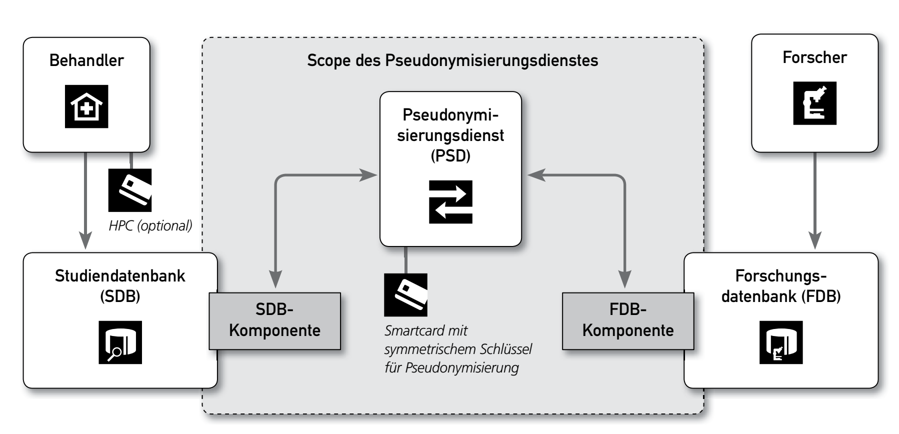


Abb. 13 Vorhandene Komponenten des Pseudonymisierungsdienstes

Der Pseudonymisierungsdienst spezifiziert folgende technische Dienste, die von den Komponenten genutzt werden können:

- PSD-Service: Dies sind die eigentlichen Services des Pseudonymisierungsdienstes, d.h. die Umwandlung eines PID_S in ein PSN und umgekehrt.
- FDB-Service: Dies sind generische und erweiterbare Services, die die FDB-Komponente bereitstellt.
- SDB-Service: Dies sind generische und erweiterbare Services, die die SDB-Komponente bereitstellt.

- Crypter: Mit diesen Services werden Nutzdaten (MDAT, Findings) (außerhalb des Pseudonymisierungsdienstes) zur Kommunikation zwischen SDB- und FDB-Komponente ver- und entschlüsselt.

Um die Vertraulichkeit der Daten zu gewährleisten, kommen die folgenden Schlüsseltypen im Rahmen des Pseudonymisierungsdienstes zum Einsatz:

- https-Keys (asymmetrische und symmetrische Schlüssel) für die SSL-Verschlüsselung,
- MDAT-Keys (asymmetrische Schlüssel) für die Datenverschlüsselung, die dem Pseudonymisierungsdienst selbst nicht bekannt sind,
- Pseudonymisierungsschlüssel (symmetrischer Schlüssel auf Smartcard).

Zur Pseudonymisierung wird ein symmetrischer kryptographischer Algorithmus hoher Sicherheit genutzt. Der Schlüssel ist gegen Auslesen gesichert auf einer Smartcard oder in einem Hardware Security Module gespeichert, deren wenige Exemplare von den für den Pseudonymisierungsdienst verantwortlichen Personen verwahrt und eingesetzt werden. Die Transformation des PID_S in ein PSN wird auf dieser Chipkarte durchgeführt, so dass der geheime Schlüssel die Karte nicht verlässt. Das Gleiche gilt für den umgekehrten Weg, bei dem ein PSN in einen PID_S transformiert wird.

Als Algorithmus wird mindestens DES-3 (Data Encryption Standard) vorgeschlagen, der in vielen marktgängigen Kartenchips implementiert ist; soweit von den Produkten her möglich, sollte der neue AES (Advanced Encryption Standard) genutzt werden (s. Kap. 2.2 des Kryptographischen Gutachtens im Anhang[31]).

Hinweis auf Weiterentwicklungsbedarf: Die Komponente Pseudonymisierungsdienst muss von zwei unterschiedlichen Ausgangskomponenten angesprochen und genutzt werden können. Sowohl aus der Klinischen Datenbank (KDB) wie aus einer Studiendatenbank (SDB) heraus muss eine weitere Pseudonymisierung angestoßen werden können, um Daten an die Forschungsdatenbank zu exportieren. Die aktuelle Implementierung sieht das Szenario eines Exports aus der KDB nicht vor und muss entsprechend erweitert werden. Zudem sollte die Vermittlung der MDAT optional auch ohne vollständige Durchleitung durch den PSD-Service möglich sein. Hierfür sollte ein entsprechendes Handling von Zugriffstickets vorgesehen werden (s. Abb. 9).

Folgende Komponenten müssten angepasst werden:

- PSD-Service: Es muss ermöglicht werden, dass dieser Service nicht nur vom SDB-Service und FDB-Service angesprochen werden kann, sondern auch von dem neu zu konzipierenden KDB-Service. Zudem muss er das Management von Zugriffstickets für die direkte Weitergabe von MDAT vom SDB- oder KDB-Service an den FDB-Service unterstützen.

31 Anhänge siehe www.tmf-ev.de/datenschutz-leitfaden

- KDB-Service: Dieser Service muss neu implementiert werden und analog zum bestehenden SDB-Service Aktionen ausführen. Wegen der unterschiedlichen Handhabung des PID_K (nicht in der KDB bekannt) muss in diese Komponente auch eine Kommunikation mit der Patientenliste, insbesondere die Handhabung eines Zugriffstickets (TKT), eingebaut werden, siehe Abbildung 14.
- SDB-Service: Hier ist eine Erweiterung insofern nötig, als dieser sowohl über einen SIC als auch über einen PID_S angesprochen werden können muss. Zudem ist das Handling von Zugriffstickets bei der direkten Versendung von MDAT an den FDB-Service umzusetzen.

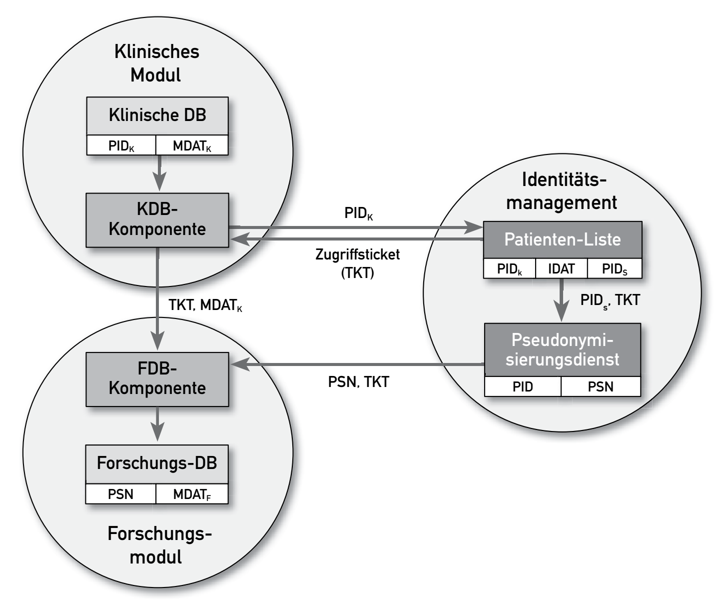


Abb. 14 Die KDB-Komponente des Pseudonymisierungsdienstes. TKT = Zugriffsticket

Ferner sollte die Implementation so gestaltet werden, dass im Maximalmodell von einem Prüfarzt des Studienmoduls, der gleichzeitig als behandelnder Arzt im Klinischen Modul wirkt, Daten aus beiden Modulen in einem Arbeitsgang an die FDB übermittelt werden können.

6.1.6.3 Übertragungssicherheit

Für die Übertragung aller relevanten Datenströme über das Internet ist ein geeignetes kryptographisches Protokoll zu nutzen. Für die meisten Anwendungsfälle (webbasierte Kommunikation oder Web-Dienste) ist SSL/TLS geeignet; es können aber auch sichere Lösungen auf VPN-Techniken aufgesetzt werden, siehe Kapitel 3.7 des Kryptographischen Gutachtens im Anhang.[32]

32 Anhänge siehe www.tmf-ev.de/datenschutz-leitfaden

6.1.7 Einordnung der bisherigen Datenschutzkonzepte der TMF

Die bisherigen Datenschutzkonzepte – die Modelle A und B des generischen Datenschutzkonzepts sowie das Datenschutzkonzept für Biomaterialbanken – ordnen sich in die im Maximalmodell beschriebenen Strukturen so ein, wie es Abbildungen 15–17 skizzieren.

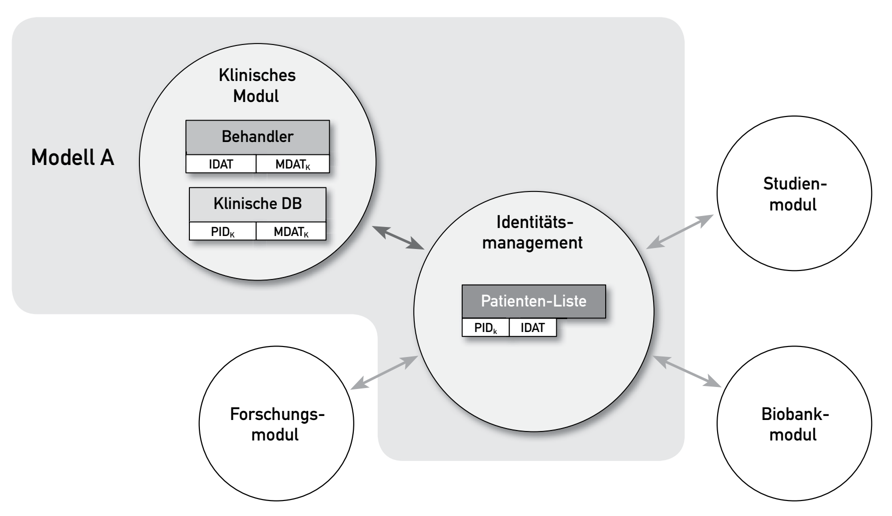


Abb. 15 Das Modell A des bisherigen generischen Datenschutzkonzepts in der übergeordneten Struktur

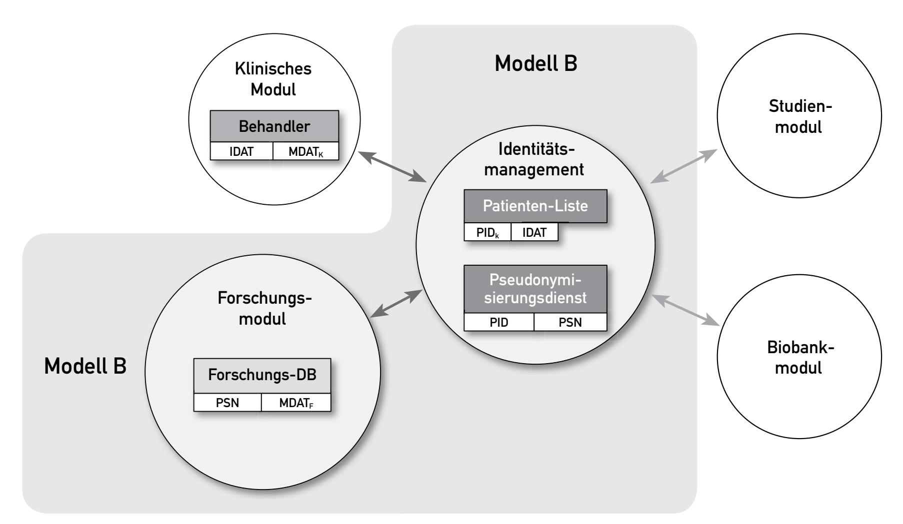


Abb. 16 Das Modell B des bisherigen generischen Datenschutzkonzepts in der übergeordneten Struktur. Für die Dateneingabe ist der Behandler aus dem Klinischen Modul nur beispielhaft dargestellt.

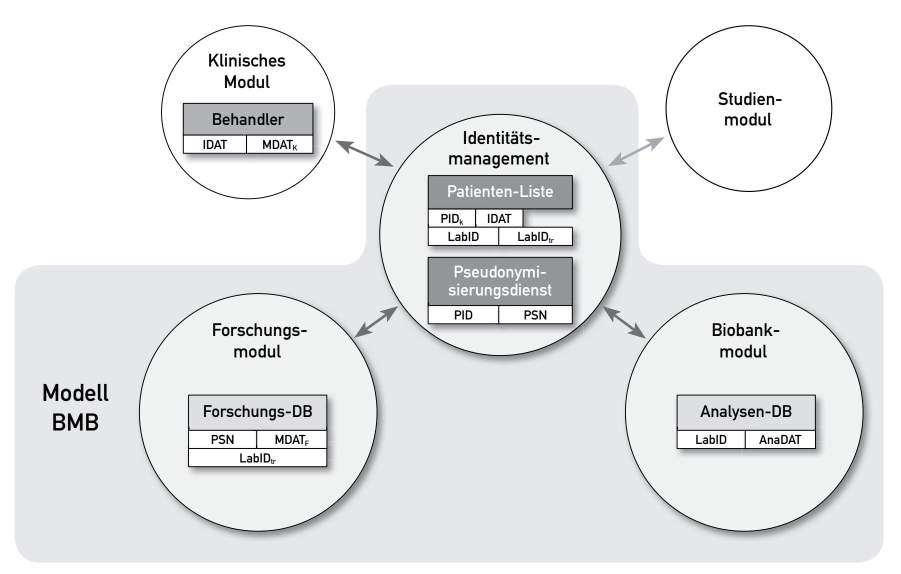


Abb. 17 Das generische Datenschutzkonzept für Biomaterialbanken in der übergeordneten Struktur. Für die Dateneingabe ist der Behandler aus dem Klinischen Modul nur beispielhaft dargestellt.

6.2 Rechtemanagement

Das Rechtemanagement betrifft die Mitarbeiter und Nutzer des Forschungsverbunds und soll u.a. gewährleisten, dass Informationen über Patienten und Studienteilnehmer nicht von Unberechtigten gesehen oder geändert werden können. Das Rechtemanagement bezieht sich auf die im Forschungsverbund eingesetzten IT-Systeme und besteht aus den Teilen:

- Authentisierung, d.h. manipulationssicherer Nachweis von Nutzer-Identitäten sowie
- Autorisierung, d.h. Vergabe von Zugriffsrechten auf Daten und von Ausführungsrechten für Funktionen.

Ist die sichere Authentisierung eines Nutzers gewährleistet, kann seine Autorisierung zur Ausübung von Funktionen im Netz und zum Datenzugriff anhand von Zugriffskontrolllisten und ähnlichen Mechanismen, die in der Regel in einem Datenbank- oder Studiensoftware-System implementiert sind, zuverlässig überprüft werden.

Das Rechtemanagement für die IT-Systeme eines Forschungsverbundes beruht auf dem Regelwerk des Forschungsverbundes, das in Policies ausgedrückt wird. In diesem Kapitel wird nur der technische Aspekt behandelt; auch dafür können nur einige grundsätzliche Aspekte beschrieben werden. Die Details der Umsetzung können sich sehr unterscheiden und sind Gegenstand des Sicherheitskonzepts des Forschungsverbunds. Grundsätzlich wird empfohlen,

- Policies zentral für einen Forschungsverbund und
- konkrete Zugriffsrechte dezentral in den einzelnen Modulen oder Datenbanken des Forschungsverbunds

zu verwalten; diese Aufteilung erscheint sowohl vom Arbeitsaufwand als auch im Hinblick auf die informationelle Gewaltenteilung zweckmäßig.

6.2.1 Zweck und Verwendungsbereich

6.2.1.1 Authentisierung von Nutzern

Authentisierung bedeutet, dass ein Nutzer seine behauptete Identität zweifelsfrei nachweist (sich ausweist); Authentifizierung, dass dieser Nachweis manipulationssicher überprüft wird (s. Abb. 18). Ein bekannter Authentisierungsmechanismus ist die Eingabe eines – zur Benutzerkennung passenden – Passworts, das im System (meist einweg-verschlüsselt) hinterlegt sein muss. Von starker Authentisierung spricht man, wenn stattdessen eine kryptographische Infrastruktur mit der Möglichkeit zur digitalen Signatur verwendet wird (s. Tab. 3); die Passwort-Eingabe wird dabei durch das digitale Signieren eines einmaligen Zufallswertes ersetzt (Challenge-Response-Verfahren), siehe Kapitel 3.6 des Kryptographischen Gutachtens im Anhang[33]. Niemand anders als der Besitzer des privaten Signaturschlüssels kann die korrekte Signatur erzeugen, und ein Angreifer kann mit dem erlauschten Zufallswert und der zugehörigen Signatur nichts anfangen. Dieses Verfahren wird typischerweise mit Smartcards realisiert. Ähnlich sicher kann die Authentisierung mit Hilfe von Hardware-Token gestaltet werden, die Einmal-Passwörter erzeugen.

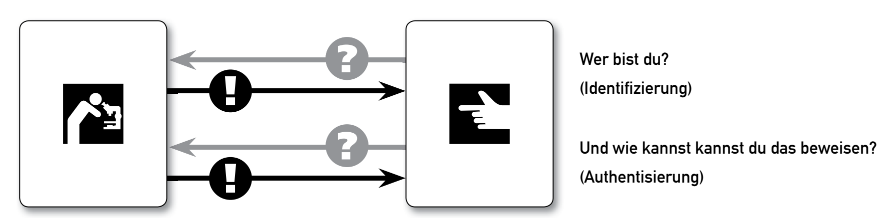


Abb. 18 Authentisierung

Tab. 3 Vergleich von schwacher und starker Authentisierung

	Frage	
Antwort bei …	**Wer bist Du?**	**Wie kannst Du das beweisen?**
Passwortverfahren (schwache Authentisierung)	Name	Passwort
Challenge-Response (starke Authentisierung)	Name (Zertifikat)	digitale Signatur

33 Anhänge siehe www.tmf-ev.de/datenschutz-leitfaden

Andere Authentisierungsverfahren, die auf der Überprüfung von biometrischen Merkmalen beruhen, sind in vernetzten IT-Systemen nicht ohne Weiteres praktikabel, da eine zentrale Datenbank dieser Merkmale mit sehr hohem Sicherheitsanspruch betrieben werden müsste. Für lokale Authentisierungsvorgänge sind aber insbesondere Fingerabdruckscanner durchaus geeignet, z.B. um Nutzer an ihrem Arbeitsplatzrechner oder für die Nutzung ihrer Smartcard zu authentifizieren. Die Marktentwicklung in diesem Bereich sollte beobachtet werden.

6.2.1.2 Rollen und Rechte im Forschungsverbund

Aufgrund einer sicher vollzogenen Authentifizierung eines Nutzers wird seine Autorisierung zur Ausübung von Funktionen im Netz zuverlässig anhand von Rechtedefinitionen festgelegt, die in Policies und Rollenbeschreibungen formuliert und in Zugangskontrolllisten o.ä. abgelegt sind.

Rechte im Forschungsverbund betreffen

- Datenzugriffe und die Verarbeitung von Daten sowie
- die Administration der IT-Systeme und der Infrastruktur mit ihren Komponenten.

Rechte sind in der Regel an Rollen gebunden, wie z.B. „Forscher“, „Systemadministrator der Forschungsdatenbank“, und werden an Einzelpersonen über deren Zuordnung zu Rollen vergeben. Die für die einzelnen Module und Komponenten eines Forschungsverbunds relevanten Rollen und Rechte werden jeweils dort beschrieben.

Ein zentrales Nutzer- und Rollenverzeichnis (z.B. Active Directory) kann für die Rechte- und Rollenverwaltung gute Dienste leisten, erscheint aber in einem verzweigten und heterogenen Forschungsverbund kaum mit angemessenem Aufwand realisierbar. Daher wird empfohlen, Regelwerke in Form von Policies zentral (als Texte) zu verwalten und in jeweils dezentraler Nutzerverwaltung und Rechtevergabe umzusetzen. Die für bestimmte Zugriffsentscheidungen benötigten ADAT werden im generischen Fall in der Patientenliste, u.U. aber auch bei den MDAT gespeichert, siehe Kapitel 6.1.5.1 und 6.5.2.4.

6.2.1.3 Zugriffsentscheidungen

Um eine Zugriffsentscheidung treffen zu können, muss das jeweilige IT-System oder der Netzdienst folgende Informationen zur Verfügung haben:

- Identität des Zugreifenden (authentifiziert),
- Rolle des Zugreifenden,
- Definition der Rechte, die mit diesem Nutzer und dieser Rolle verbunden sind.

Für die Verwaltung der Zugriffsrechte auf Objekte (IT-Systeme oder Netzdienste, Daten oder Prozesse) gibt es prinzipiell verschiedene Ansätze (s. Abb. 19):

1. Objekte (bzw. die sie tragenden IT-Systeme) verwalten sich selbst, d.h., sie prüfen bei einer Anfrage eines authentifizierten Partners (Person oder Prozess) anhand der in ihnen selbst implementierten Regeln, wie sie antworten oder reagieren wollen. Ein solcher dezentraler Ansatz benötigt nur ein Minimum an Vertrauensannahmen (nämlich in die zuverlässige Authentisierung), stößt aber sehr schnell an Komplexitätsgrenzen.
2. Es werden vertrauenswürdige Dienste genutzt, die die Entscheidung auf sichere Weise treffen und übermitteln können; dies kann wiederum auf zwei Weisen geschehen:
   - online durch Abfrage eines TTP-Dienstes, der eine Entscheidung der Art „erlaubt“ oder „nicht erlaubt“ zurückliefert,
   - offline, durch Prüfung eines „Credentials“, also eines von einem TTP-Dienst signierten Attributs (Zugriffsticket), das die Berechtigung ausdrückt und vom Antragsteller präsentiert wird.

Beispiele: Die Patientenliste enthält auch die Information, wer als zugriffsberechtigter behandelnder Arzt für einen Patienten beim Forschungsnetz erfasst ist (ADAT, s. Kap. 6.1.1.1). Diese Information kann z.B. an eine Klinische Datenbank (KDB) weitergegeben werden. Rechte, die in einer Studiendatenbank (SDB) festgelegt sind, können an andere Anwendungen im Forschungsverbund mitgeteilt werden.

6.2.2 Anwendungsfälle

6.2.2.1 Anwendungsfälle und ihre empfohlene Lokalisierung

Tabelle 4 stellt dar, welche Lokalisierungen für die verschiedenen Anwendungsfälle empfohlen werden.

Tab. 4 Lokalisierung von Anwendungsfällen

Anwendungsfall	empfohlene Ansiedlung
Anlegen und Administrieren von Nutzerkonten	dezentral, evtl. in zentralem Verzeichnis
Anlage und Verwaltung von Rollen	zentral oder dezentral nach zentral vorgegebenen Policies
Zuordnung von Nutzern zu Rollen	dezentral
Definition von Policies	zentral
Definition von Rechten	dezentral
Zuordnung von Rechten zu Rollen	zentral oder dezentral
Verteilung der Nutzer- und Rechtedaten an Subsysteme (z.B. einzelne Datenbanken)	von zentral nach dezentral, evtl. auch von dezentral nach dezentral
Prüfung von Rechten	dezentral, evtl. durch zentrale Dienste unterstützt

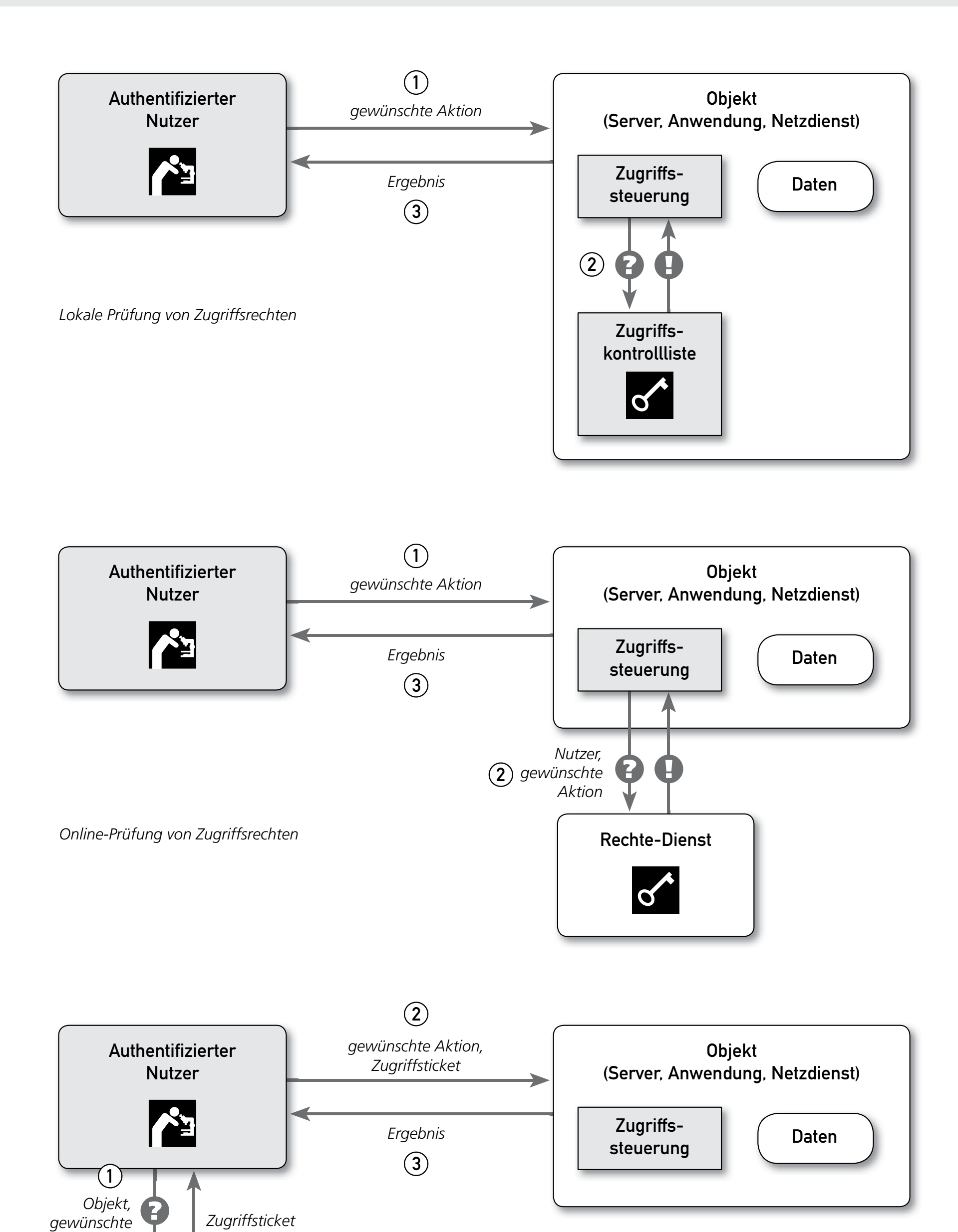


Abb. 19 Drei Modelle der Zugriffsentscheidung

Als Anwendungsfälle kommen, je nach konkreter Implementierung, die Verwaltung von zentralen Diensten sowie der Datenbanken im Forschungsverbund und evtl. einer PKI hinzu.

6.2.2.2 Benötigte Dienste

Falls das Rechtemanagement im Forschungsverbund überhaupt zentral organisiert wird, sind eine Reihe von Sicherheitsdiensten nötig, die als Trusted Third Party Services aufzusetzen sind, d.h. – vom technischen Standpunkt aus betrachtet – als Netzdienste oder Web-Services, die sowohl interaktiv als auch von Prozessen in Anspruch genommen werden können und das Vertrauen aller am Netz Beteiligten genießen. Die wichtigsten davon sind

- Benutzerverwaltung,
- PKI- und Zertifikateverwaltung,
- Authentisierungsdienst,
- Rollenverwaltung, in der Regel in Form von Benutzergruppen, mit dezentraler Zuordnung von Benutzern zu Rollen,
- Policy-Dienste: Definition, Pflege und Interpretation von Sicherheitsrichtlinien, die vor allem Zugriffsberechtigungen betreffen und durch generische Zugriffsregeln ausgedrückt werden,
- Zugriffskontroll- oder Autorisierungsdienste: konkrete Umsetzung der Policies in Zugriffsentscheidungen (auch dynamische und kontextsensitive, Workflow-abhängige),
- Gateways zwischen Modulen oder Teilbereichen mit unterschiedlichen Policies.

6.2.3 Nutzer, Rollen und Rechte

6.2.3.1 Generische Rollen im Forschungsverbund

Die durch die primären Aufgaben des Forschungsverbunds definierten Rollen (behandelnder Arzt, Prüfarzt, Studienleiter, Forscher) sind bei den einzelnen Modulen definiert; siehe auch das Glossar.

Daneben gibt es eine Reihe von implementationsabhängigen, durch die IT-Architektur des Forschungsverbundes definierten Rollen, hauptsächlich Systemadministratoren und Nutzer für die eingerichteten Dienste und Datenbanken; diese werden im jeweiligen Kontext beschrieben.

6.2.3.2 Rollen im Rechtemanagement

Hier gibt es die Rolle der Systemverwalter für alle separat betriebenen zentralen Komponenten, z.B. für ein zentrales Verzeichnis, sowie zur dezentralen Rechteverwaltung auf Servern und für Dienste.

6.2.3.3 Mögliche Rollenkonflikte

Einzelne klinisch tätige Ärzte sind gleichzeitig auch als Wissenschaftler in ihren jeweiligen Forschungsnetzen tätig; dabei besteht das Risiko, dass ein solcher Arzt Daten von einem seiner früheren Patienten, der inzwischen bei einem anderen Arzt in Behandlung war, trotz Pseudonymisierung wieder erkennt und somit unbefugt Informationen erhält. Dieser interpersonelle Konflikt ist jedoch nicht neu, auch bei der konventionellen Papierdokumentation in der klinischen Forschung bestehen ähnliche Probleme, wobei die Wiedererkennbarkeit sogar erleichtert ist. Zudem sind hier die Zugriffsregeln nicht elektronisch einstellbar, so dass die Regel „wenig Zugriff ist voller Zugriff" bei der konventionellen Datenhaltung zutrifft. Im elektronischen Verfahren lässt sich die Behandlung der „Doppelrolle" durch eine rollenbasierte Zugriffsberechtigung, die in diesem Fall zwei unterschiedliche Profile für einen Mitarbeiter vorsieht, regeln. Ein bewusster, vorsätzlicher Missbrauch dieses Konzeptes – wie auch bei der Papierlösung – lässt sich aber naturgemäß nicht restlos verhindern, und ist durch die ärztliche Schweigepflicht sowie durch die Regeln des Forschungsverbundes auszuschließen. Hier sei auch auf das Rechtsgutachten [11] verwiesen. Ähnliches gilt, wenn Arzt und Systemadministrator in einer Person verkörpert werden.

Weiter kann ein Rollenkonflikt entstehen, wenn eigentlich getrennt zu haltende Datenbestände wie z.B. identifizierende Daten (IDAT) und medizinische Daten (MDAT) in derselben Institution gespeichert werden und Zugriffe von Mitarbeitern auf beide Datenbestände nicht sicher genug ausgeschlossen werden können. In solchen Fällen ist kritisch zu prüfen, ob eine solche Vereinfachung nach den Kriterien der Verhältnismäßigkeit (vgl. Kap. 6.7) vertretbar ist. Gerade in großen Forschungsverbünden, die das hier vorgeschlagene Maximalmodell implementieren und je Modul ggf. auch über mehrere Datenbanken verfügen, ist eine besonders sorgfältige Prüfung auf mögliche Rollenkonflikte bei allen Beteiligten unumgänglich.

6.2.4 Verantwortlichkeiten

Für die grundsätzliche Definition von Rechten und Policies ist die Leitung des Forschungsverbundes zuständig. Diese Aufgabe kann an den Ausschuss Datenschutz delegiert werden.

Die Dienste für das Rechtemanagement nach Kapitel 6.2.2.2 können zentral oder dezentral angeordnet werden. Bei zentraler Anordnung besteht noch die Wahl zwischen einer am Netz beteiligten Einrichtung und einem externen Dienstleister. Wie solche TTP-Dienste rechtlich und organisatorisch aufgesetzt werden, hängt vom rechtlichen und organisatorischen Status der Anwendungsumgebung ab. Für ein medizinisches Forschungsnetz wird man rechtlich oder vertraglich verpflichtete Organisationen wählen, die ein hohes Sicherheitsniveau garantieren können.

Das Nutzer- und Rechtemanagement ist in hohem Maße abhängig von bestehenden Infrastrukturen und Workflows in den Forschungsnetzen. Es wird aber jedenfalls von allen Modulen vorausgesetzt und benutzt. Da das Identitätsmanagement an zentraler Stelle im Forschungsverbund steht, liegt es nahe, die zentralen Funktionen des Rechtemanagements ebenfalls hier anzusiedeln. In einem großen Forschungsverbund ist eine Trennung der Funktionen im Sinne der informationellen Gewaltenteilung zu empfehlen. Hier ist aber, abhängig von Größe und Struktur des Forschungsverbundes, die Verhältnismäßigkeit des Aufwandes zu wahren. Unter dem Gesichtspunkt des Datenschutzes können sowohl zentrale als auch dezentrale Lösungen sicher gestaltet werden.

6.2.5 Aspekte der Realisierung

In der Praxis gibt es für das Rechtemanagement und seine Komponenten viele unterschiedliche technische Lösungen; keine davon ist als allgemein etablierter Standard anzusehen. Am weitesten verbreitet dürfte nach wie vor ein separates Rechtemanagement in jeder selbstständig administrierten Komponente eines Forschungsverbundes sein, in der Regel mit Passwort-basierter Authentisierung auf jedem einzelnen Server, sowie die in der jeweiligen Datenbank vorgesehene Regelung von Zugriffsrechten; dies ist aufgrund der Marktdominanz dieser Verfahren bei weitem am einfachsten umzusetzen. Daher ist das Rollenmanagement auf der Seite der konkreten Implementierung in der Regel nicht als Modul oder Komponente abgrenzbar.

Dennoch wird empfohlen, die Verwaltung von Nutzern bei geeigneten Ressourcen möglichst zentral zu organisieren, auf jeden Fall aber die Definition von Policies und möglichen Rollen. Allerdings sollen die Rechte für jeden Teil der Infrastruktur gesondert administriert werden können: Die in diesem Konzept an vielen Stellen geforderte informationelle Gewaltenteilung wird nur wirksam umgesetzt, wenn die disziplinarisch unabhängigen Stellen im Netz über die jeweilige Rechtevergabe selbst wachen. Dies impliziert insbesondere die Zuordnung von Nutzern zu Rollen auf der Ebene der einzelnen Module. Zur Nutzerverwaltung und Rollenvergabe werden also dezentrale Zugriffsrechte benötigt.

6.2.5.1 Nutzung eines Verzeichnisdienstes

Als zentrale Komponente dafür wird ein Verzeichnisdienst (Directory) empfohlen, der aber dezentralen Systemadministratoren für die Verwaltung ihrer jeweiligen Nutzer zugänglich ist. Dieser ermöglicht eine zentrale Authentisierung (Single-Sign-On). Unter dem Gesichtspunkt des Datenschutzes ist aber eine völlig dezentrale Nutzerverwaltung ebenso akzeptabel.

6.2.5.2 Nutzung einer PKI

Die Public-Key-Infrastruktur (PKI) sorgt für ein sicheres Management privater und öffentlicher Schlüssel. Für den privaten Schlüssel – der ja als persönliches Geheimnis zu behandeln ist – ist ein sicherer Aufbewahrungsort vorzusehen, den der Schlüssel möglichst nicht verlassen muss. Ideal geeignet ist eine Chipkarte (Smartcard), die auch in der Lage ist, die kryptographischen Grundfunktionen Verschlüsselung, Signatur und starke Authentisierung auszuführen.

Öffentliche Schlüssel müssen dagegen nicht geheim gehalten werden, aber ihre Authentizität muss gesichert werden. Dazu dienen Zertifikate. Sie setzen voraus, dass eine von allen Teilnehmern anerkannte vertrauenswürdige Zentralinstanz existiert, die durch digitale Signatur den öffentlichen Schlüssel an eine eindeutige Kennzeichnung seines Besitzers bindet. Eine solche Instanz wird Trustcenter oder Certification Authority (CA) genannt und ist ein Beispiel für eine Trusted Third Party (TTP).

Aufbau und Betrieb einer PKI sind Standardaufgaben, zu denen es zahlreiche bestehende Verfahrensvorschriften und Softwareprodukte gibt. Für medizinische Forschungsverbünde wird aber empfohlen, keine eigene PKI aufzubauen, sondern mittelfristig die der zukünftigen Gesundheitstelematik, insbesondere den Heilberufeausweis (HBA) zu nutzen. Die Möglichkeiten hierzu folgen aus dem Rechtsgutachten von Roßnagel und Mitarbeitern [11].

6.2.5.3 Technische Aspekte der Rechtevergabe

Wird mit einem rollenbasierten Ansatz gearbeitet, so ist keine explizite Verteilung von Rechtedaten nötig. Die Zuordnung von Nutzern zu Rollen wird in der Nutzerverwaltung dezentral (selbst wenn es ein zentrales Nutzerverzeichnis gibt) durchgeführt, das rollenbasierte Rechtemanagement wird lokal an den Servern auf der Basis der netzweit geltenden Policies eingestellt.

Für die Verteilung der Rechte-Informationen geeignete Methoden und Werkzeuge werden nachfolgend aufgeführt. Solche Informationen können entweder als Zugriffsentscheidung auf geschütztem Wege von einem zentralen Server an die jeweiligen Dienste oder Datenbanken übermittelt werden, oder der jeweilige anfragende Nutzer erhält diese in Form eines Credentials (Zugriffstickets), d.h. einer vom zentralen Dienst digital signierten „Erlaubnisbescheinigung“.

6.2.5.4 Spezifikation von Richtlinien und Regeln

Richtlinien und Regeln eines medizinischen Forschungsverbundes werden in der Regel in Textform beschrieben und dezentral in den einzelnen Modulen und Komponenten entsprechend implementiert. Für große und komplexe Verbünde kommt aber auch die Einführung und Nutzung von technischen Werkzeugen in Betracht, wenn sich der Investitionsaufwand hierfür lohnt.

Wichtige entsprechende Werkzeuge für die Einrichtung von Sicherheitsdiensten sind standardisierte Sprachen, mit denen Richtlinien und Regeln eindeutig spezifiziert und automatisiert verarbeitet werden können; gängige Ansätze hierfür sind z.B.

- SAML = Security Assertion Markup Language, eine XML-basierte Auszeichnungssprache zur Beschreibung von sicherheitsbezogenen Informationen.
- XACML = eXtensible Access Control Markup Language: ein XML-Schema, das die Verwaltung von Policies (im engeren Sinne: Rechtevergaberegeln) definiert. XACML definiert eine Sprache, in der Zugriffsberechtigungen durch Attribute, Bedingungen und Regeln ausgedrückt und zwischen verschiedenen Diensten und Prozessen kommuniziert werden können. Dadurch lassen sich wesentlich komplexere Zugriffsregeln ausdrücken als durch einfache Zugriffslisten (ACL = Access Control List).

6.2.5.5 Weitere mögliche Werkzeuge

Auch hier handelt es sich um eine Aufzählung von Werkzeugen, deren Nutzung einer Aufwands- und Nutzenabschätzung unterliegt und die nicht generell für alle Forschungsverbünde empfohlen wird.

- Kerberos ist ein verteilter Authentisierungsdienst für Computernetze.
- Shibboleth ist eine Sammlung von Diensten, die lokalen Authentisierungs- und Autorisierungsdiensten ermöglicht, fremden Diensten die nötigen Informationen für Zugriffsentscheidungen zur Verfügung zu stellen
- VOMS (Virtual Organization Membership Service) ist ein datenbankgestützter Mechanismus zur zentralen Verwaltung von Rollen und Rechten (globale Autorisierung)

Hinweis: Erfahrungen mit dem Einsatz solcher Werkzeuge liegen bisher nur im Grid-Umfeld vor. Die Nutzbarkeit für medizinische Forschungsverbünde müsste erst noch in einem Pilotprojekt geprüft werden, bevor konkrete Empfehlungen zum Einsatz formuliert werden können.

6.3 Kombinierter Einsatz von Studienmodul und Klinischem Modul

6.3.1 Zweck und Anwendungsbereich

In den Kapiteln 5.1 und 5.2 werden die Konzepte eines Klinischen Moduls zur versorgungsnahen Datenerhebung sowie eines Studienmoduls zur Durchführung einzelner Forschungsprojekte (z.B. klinischer Studien) getrennt voneinander beschrieben. Im Folgenden soll der kombinierte Einsatz eines Klinischen Moduls und eines Studienmoduls innerhalb eines Forschungsnetzwerks dargestellt werden. Die Module werden hierbei auf Basis der im jeweiligen

Kapitel beschriebenen Konzepte eingesetzt. Abweichungen sowie Besonderheiten im Zusammenspiel der Module werden zusätzlich beschrieben.

Im Rahmen seltener sowie chronischer Erkrankungen kann sich die Notwendigkeit ergeben, Patienten längerfristig im Rahmen eines Forschungsnetzes zu behandeln. Hierdurch wird zum einen die Möglichkeit zur kontrollierten longitudinalen Erhebung und Auswertung von Daten geschaffen, zum anderen können Patienten auf Basis der im Rahmen der Versorgung erhobenen Daten für Studien im Rahmen des Forschungsnetzes rekrutiert werden. Es entstehen Überschneidungen zwischen den im Rahmen der Routineversorgung und für die Studiendokumentation benötigten Daten, die sowohl zum Vorteil des Patienten aus der Forschung in die Versorgung übernommen (z.B. Nutzung eines aufwändigen Bildgebungsverfahrens für die Versorgung) als auch zur Vermeidung einer Mehrfacherfassung von der Versorgung in die Forschung übertragen werden können. Voraussetzung ist das Vorliegen der Daten in einer für den jeweiligen Anwendungszweck notwendigen Qualität und Vollständigkeit.

Durch die Verbindung von Studien- und Klinischem Modul ergeben sich zusätzliche Datenflüsse für die Datenübernahme, die sowohl bei der Umsetzung dieser Komponenten als auch beim ID-Management berücksichtigt werden müssen.

Im Rahmen des Zusammenflusses von Studien- und Versorgungsaspekten kann sich auch eine Personeneinheit von Studienarzt und behandelndem Arzt ergeben. Die Zugriffsrechte ergeben sich dabei aus der Vereinigungsmenge der beiden Rollen. Um Doppelerfassungen zu vermeiden, sollte nach Möglichkeit die Eingabe über ein System erfolgen, von dem aus die Daten geschützt an das jeweilige andere System übertragen werden.

Informationssysteme der Routineversorgung (z.B. Krankenhausinformationssysteme, Praxisverwaltungssysteme oder elektronische Patientenakten) können Bestandteile eines Klinischen Moduls sein. Ebenso können Daten aus separat betriebenen Routineversorgungssystemen mit dem Klinischen Modul ausgetauscht werden. Das generische Datenschutzkonzept der TMF deckt in diesen Fällen nur die zweckgebundene Nutzung im Kontext des Klinischen Moduls ab, es soll kein allgemeines Datenschutzkonzept für den Betrieb von Systemen der klinischen Routineversorgung abgebildet werden.

6.3.2 Anwendungsfälle und Prozesse

Die Anwendungsfälle des Studien- und des Klinischen Moduls werden ausführlich in den entsprechenden Kapiteln beschrieben. In diesem Kapitel wird der Fokus auf die Prozesse gelegt, die sich aufgrund der Verbindung des Studienmoduls mit dem Klinischen Modul ergeben.

6.3.2.1 Daten zwischen Studienmodul und Klinischem Modul übermitteln

Wenn ein Patient eines Forschungsverbundes sowohl an einer Studie als auch am Klinischen Modul teilnimmt, so besteht die Möglichkeit, die schon in einem Modul erfassten Daten des Patienten in das andere Modul zu übertragen, um Doppelerfassungen zu vermeiden. Um diese Übertragung zu ermöglichen, bedarf es eines netzweiten Identitätsmanagements (s. Kap. 6.1), das sowohl das Pseudonym des Patienten aus dem Klinischen Modul (PID_K) als auch das aus dem Studienmodul (PID_S bzw. SIC_S für jede Studie) enthält.

Bei der Übertragung aus dem Studienmodul in das Klinische Modul werden zwei Fälle unterschieden:

a) Der verantwortliche Arzt stellt eine entsprechende Anfrage von Seiten des Klinischen Moduls an das Studienmodul (s. dazu auch Abb. 20). Hierzu schickt er eine Nachricht mit den identifizierenden Daten des Patienten an das Identitätsmanagement. Das Identitätsmanagement authentifiziert und autorisiert den Arzt, selektiert anhand der identifizierenden Daten des Patienten die Pseudonyme PID_K und PID_S bzw. SIC und erstellt ein Zugriffsticket (TKT). Das TKT wird mit dem PID_K des Patienten an das Klinische Modul und mit dem PID_S bzw. SIC an das Studienmodul geschickt. Das Studienmodul selektiert anhand des PID_S bzw. dem SIC die medizinischen Daten ($MDAT_S$) des Patienten, entfernt den PID_S bzw. den SIC und schickt die Daten mit dem TKT an das Klinische Modul. Das Klinische Modul ordnet den Datensatz anhand des TKT dem PID_K des Patienten zu und speichert die Daten zu dem entsprechenden PID_K.

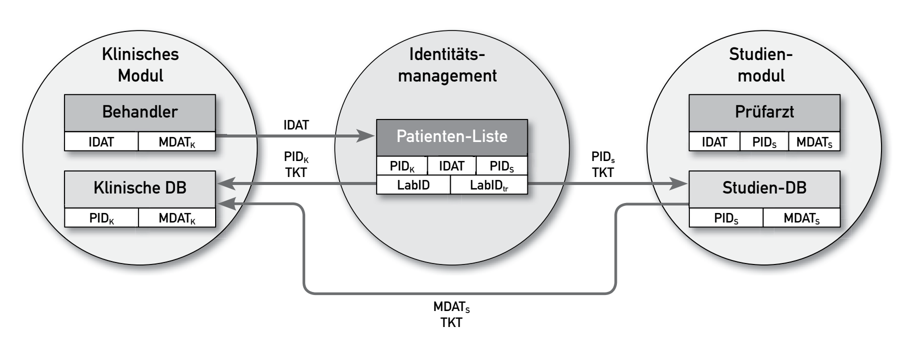


Abb. 20 Transfer von medizinischen Daten eines Patienten aus dem Studienmodul in das Klinische Modul, angestoßen vom Klinischen Modul.

b) Der Datentransfer wird auf Seiten des Studienmoduls angestoßen (dies kann beispielsweise nach Abschluss einer Studie automatisch erfolgen, s. dazu auch Abb. 21). Hierzu muss der PID_S des entsprechenden Patienten an das Identitätsmanagement geschickt werden. Das Identitätsmanagement authentifiziert und autorisiert den entsprechenden Anfragenden, ordnet dem PID_S des Patienten seinen PID_K zu und erstellt ein Zugriffsticket. Das TKT wird mit dem

PID_K des Patienten an das Klinische Modul geschickt und mit dem PID_S an das Studienmodul. Die Selektion und Übertragung erfolgt wie oben bereits beschrieben.

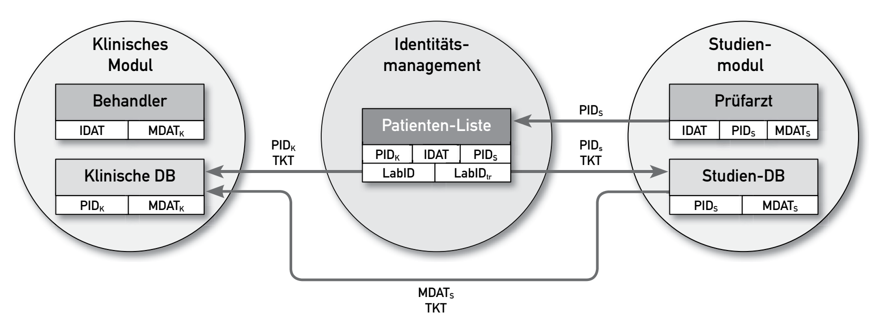


Abb. 21 Transfer von medizinischen Daten eines Patienten aus dem Studienmodul in das Klinische Modul, angestoßen vom Studienmodul.

Die Übertragung aus dem Klinischen Modul an das Studienmodul kann auch aus beiden Richtungen angestoßen werden. Die Mechanismen sind ebenfalls die gleichen. Die Übertragung der Daten des Patienten erfolgt in diesem Fall vom Klinischen Modul an das Studienmodul.

Ziel der Verwendung eines durch das Identitätsmanagement vermittelten Zugriffstickets ist es, eine Verknüpfung von PID_K und PID_S bzw. SIC außerhalb der Patientenliste zu verhindern. Eine direkte Kommunikation der medizinischen Daten des Patienten (in verschlüsselter Form) über die Patientenliste und damit die Möglichkeit, die Pseudonyme direkt in den medizinischen Daten auszutauschen (angelehnt an das Verfahren des Pseudonymisierungsdienstes), wurde nicht gewählt, um die klare räumliche und organisatorische Trennung der medizinischen Daten von den identifizierenden Daten des Patienten aufrecht zu erhalten. Das oben beschriebene Verfahren wird als eine mögliche Variante zur datenschutzkonformen Übertragung medizinischer Daten eines Patienten zwischen Klinischem und Studienmodul gesehen. Sofern die gerade beschriebenen Schutzprinzipien eingehalten werden, sind auch andere Umsetzungsmöglichkeiten vorstellbar.

Eine relevante Standardisierungsinitiative für solche Datentransfers stellt das Profil Retrieve Form for Data Capture (RFD) der Organisation Integrating the Healthcare Enterprise (IHE) dar[34]. Auch wenn dieser Vorschlag auf das notwendige korrekte Handling der Pseudonyme derzeit noch nicht detailliert eingeht, könnten die hier spezifizierten Kommunikationsstandards für künftige Softwaresysteme eine wichtige Anforderung darstellen.

34 siehe http://wiki.ihe.net/index.php?title=Retrieve_Form_for_Data_Capture

6.3.2.2 Patienten in Klinisches Modul oder Studienmodul aufnehmen

Beim Einholen der Einwilligungserklärung sollte mit abgefragt werden, ob der Patient auch an möglichen Studien Interesse hat bzw. später auf entsprechende Studien hingewiesen werden möchte. Des Weiteren sollte abgefragt werden, ob der Patient schon an Studien im Rahmen des Forschungsverbundes teilgenommen hat und ob diese Daten im Klinischen Modul genutzt werden sollen. Ist dies der Fall, so können die Daten wie oben beschrieben aus dem Studienmodul an das Klinische Modul übertragen werden.

6.3.2.3 Datenqualität sichern

Ergänzend zu üblichen Qualitätssicherungsverfahren in einzelnen Studien kann bei Kombination mit einem Klinischen Modul auch ein Abgleich von Daten aus der Versorgung zu einem Patienten durchgeführt werden. Sollte sich dabei z.B. herausstellen, dass sich das Geburtsjahr geändert hat oder bei einem erwachsenen Patienten eine deutlich veränderte Körpergröße festgestellt wurde, so wären dies gerechtfertigte Auslöser für eine weitere Datenüberprüfung. Aus Sicht des Klinischen Moduls können ebenfalls Daten einer Studie für die Qualitätssicherung herangezogen werden.

Sollten bei der Qualitätssicherung im Klinischen Modul Änderungen an Daten erfolgen, die ihren Ursprung im Studienmodul haben und in das Klinische Modul übernommen wurden, so sollte sichergestellt werden, dass die Verantwortlichen des Studienmoduls informiert werden. Hierbei können die entsprechend zu ändernden Daten des Patienten mit dem Hinweis auf den Fehler wie oben beschrieben zwischen dem Klinischen Modul und dem Studienmodul ausgetauscht und entsprechende Fehler korrigiert werden. Bei Korrekturen im Studienmodul wird äquivalent verfahren. Für diese Vorgehensweise müssen Datensätze, die in das jeweils andere Modul übertragen worden sind, entsprechend gekennzeichnet werden.

6.3.2.4 Daten erheben

Werden teilweise die gleichen Daten eines Patienten im Rahmen der Versorgung sowie einer Studie erfasst, so ist es sinnvoll, diese nur in einem System zu erfassen und sie anschließend im Studienmodul und Klinischen Modul zu speichern. Je nach Workflow kann hier das Studienmodul oder das Klinische Modul das erfassende System sein. Die Übertragung der Daten an das andere System kann nach dem oben beschrieben Verfahren erfolgen.

6.3.2.5 Studiendaten auswerten

Nach der Auswertung einer Studie können die entsprechenden Ergebnisse der Studie für den Patienten im Klinischen Modul bereitgestellt werden. Hierzu

werden die Ergebnisse mit dem PID_S des Patienten versehen und nach dem gleichen Verfahren wie die Studiendaten an das Klinische Modul übertragen.

6.3.2.6 Unerwartete Ereignisse managen

Sollten während einer Studie unerwartete Ereignisse zu einem Patienten eintreten, so können diese Informationen mit dem PID_S des Patienten versehen und nach dem gleichen Verfahren wie die Studiendaten an das Klinische Modul übertragen werden.

6.3.2.7 Studiendaten archivieren

Vor der Archivierung von Studien sollten die entsprechenden Daten für die Versorgung des Patienten wie oben beschrieben in das Klinische Modul übertragen werden.

6.3.2.8 Daten sperren, anonymisieren oder löschen

Bei einem Widerruf der Einwilligung eines Patienten ist zu überprüfen, ob dieser Widerruf sowohl für die Daten des Studienmoduls als auch für die Daten des Klinischen Moduls gilt und die entsprechenden Daten in den Modulen gelöscht bzw. anonymisiert werden. Des Weiteren ist eine Löschung der identifizierenden Daten im Identitätsmanagement erforderlich.

Wenn Studiendaten im Rahmen einer klinischen Prüfung nach den Vorschriften des AMG verwaltet werden, so ist bei einem Widerrufen der Einwilligung zu beachten, dass bestimmte Daten aus Sicherheitsgründen nicht gelöscht oder anonymisiert werden dürfen (vgl. Kap. 4.3.1).

6.3.2.9 Machbarkeit einer Studie prüfen und Rekrutierung unterstützen

Für das Prüfen der Machbarkeit einer Studie und mehr noch die Rekrutierungsunterstützung wird vor allem die Klinische Datenbank wichtige Daten liefern können. Zum einen wird sie mehr Datensätze als eine Studiendatenbank beinhalten, wenn in einem Forschungsverbund über einen längeren Zeitraum mehr Patienten behandelt wurden als aktuell in eine der laufenden Studien eingeschlossen sind. Wichtiger aber ist noch, dass die aktuell in Studien eingeschlossenen Patienten nicht für eine weitere Rekrutierung zur Verfügung stehen.

Die Überprüfung der Machbarkeit einer Studie anhand anonymer Fallzahlen aus der Vergangenheit kann grundsätzlich auch unabhängig von einer vorherigen Einwilligung durchgeführt werden. Problematisch wäre jedoch eine anonyme Zusammenführung von Klinischer und Studiendatenbank, die zu doppelten Datensätzen führt. Bei Vorliegen einer entsprechenden Einwilligung der Probanden und einer Genehmigung durch den Ausschuss Daten-

schutz ist grundsätzlich auch eine pseudonyme Zusammenführung der Daten zur Abschätzung der Machbarkeit neuer Vorhaben oder auch zur Rekrutierungsunterstützung möglich. Letzteres jedoch nur bei Vorliegen eines sinnvollen Nutzungsszenarios für die Daten einer Studiendatenbank zu Rekrutierungszwecken. Eine mögliche Kontaktierung des Patienten kann wie im Kapitel 6.3 beschrieben erfolgen.

6.3.3 Nutzer, Rollen und Rechte

Für die Patientenliste ist analog zur Beschreibung im Studienmodul ein Administrator, ggf. unterstützt durch eine Dokumentationskraft, vorzusehen. Für die Administration der Studiendatenbank und der Klinischen Datenbank werden separate Administratoren benötigt, die Zugriff auf die jeweils dort gespeicherten MDAT, nicht jedoch die IDAT in der Patientenliste haben. Das Administrationspersonal von ID-Management und Studiendatenbank/Klinischer Datenbank sollte unter getrennter Verantwortung stehen (organisatorische Gewaltenteilung).

Studienärzte und Dokumentationskräfte erhalten Zugang auf die von ihnen betreuten Patienten im Studienmodul. Behandelnde Ärzte wiederum erhalten Zugriff auf die von ihnen betreuten Patienten im Klinischen Modul. Eine Patientenselbsteingabe kann in das Studienmodul oder Klinische Modul erfolgen, wenn sichergestellt ist, dass ein Patient nur Zugriff auf den jeweils eigenen Datensatz erhält. Bei Personeneinheit von Studien- und behandelndem Arzt ergeben sich die Berechtigungen aus der Vereinigungsmenge der jeweiligen Rollen.

Die Umsetzung der Rollen Monitor und Sponsor erfolgt analog zur Beschreibung des Studienmoduls, wobei Quelldaten, die im Rahmen des Monitorings geprüft werden, auch im Klinischen Modul liegen können. Wenn sich aufgrund des Monitorings Änderungsbedarf an Daten des Studienmoduls ergeben, sollen diese Änderungen im Klinischen Modul nachvollzogen werden.

6.3.4 Verantwortlichkeiten

Die Verantwortlichkeiten innerhalb des Studienmoduls und Klinischen Moduls werden in den Kapiteln 5.2 und 5.1 beschrieben. Die Gesamtverantwortung liegt beim Forschungsverbund. Mit der Führung der Patientenliste sowie der Studiendatenbank /Klinischen Datenbank werden voneinander unabhängige Einheiten des Verbunds beauftragt. Analog zum Studienmodul kann die Gesamtverantwortung mit der Führung der Patientenliste auch an einen zentralen Datentreuhänder übergeben werden. Datenschutzrechtlich sensible Fragen (z.B. Depseudonymisierung) sollten in einem zentralen Gremium (Ausschuss Datenschutz) entschieden werden. Bei einer multizentrischen Erhebung in ein zentrales System müssen Verantwortliche an den beteiligten

Standorten festgelegt werden. Bei Studien gemäß AMG oder MPG sind hier geltende zusätzliche Anforderungen sowie die übergeordnete Verantwortung des Sponsors zu berücksichtigen.

6.4 Kombinierter Einsatz von Studien- und Forschungsmodul

In Kapitel 5.2 wird das technische und organisatorische Konzept für eine Infrastruktur beschrieben, die für die Durchführung einzelner Forschungsprojekte wie z.B. klinischer Studien gemäß der Vorgaben des AMG oder MPG geeignet ist. Dabei wurde lediglich angedeutet, dass auch eine weitere Nutzung der Daten nach Abschluss der Studien für bestimmte Fragestellungen notwendig sein könnte. Ebenfalls bereits beschrieben (Kap. 5.3) sind Aufbau und Rahmenbedingungen langfristig angelegter Forschungsdatenbanken, wie sie typischerweise für epidemiologische Fragestellungen, zur Generierung neuer Forschungshypothesen oder für die Rekrutierungsunterstützung genutzt werden. Dabei wurde jedoch bisher nicht näher beschrieben, wie eine übergreifende Infrastruktur in datenschutzgerechter Weise aufgebaut werden kann, die sowohl die Durchführung einzelner Studien und Forschungsprojekte wie auch die Zusammenführung der Daten nach Abschluss der Studien in einer übergeordnet und langfristig angelegten Forschungsdatenbank unterstützt. Der Schwerpunkt der folgenden Ausführungen liegt somit auf der Verzahnung von Studien- und Forschungsmodul, wie sie jeweils einzeln bereits in Kapitel 5 beschrieben wurden.

6.4.1 Zweck und Anwendungsbereich

Die vom Bundesministerium für Bildung und Forschung (BMBF) seit 1999 geförderten Kompetenznetze in der Medizin hatten und haben neben der Vernetzung von Forschung und Versorgung insbesondere auch die Einbettung einzelner Forschungsprojekte in übergeordnete Infrastrukturen zum Ziel. So sollten nicht nur die Aufwände für die Umsetzung einzelner Studien verringert, sondern aus den gesammelten Daten auch ein größerer Nutzen gezogen werden können. Dieses auch im Interesse der Patienten liegende Ziel führte über die Vermittlung und Unterstützung in der TMF zur Ausarbeitung einer generischen Konzeption, die dann als Modell B in den generischen Datenschutzkonzepten der TMF 2003 bekannt wurde [1]. Der Aspekt der Unterstützung einzelner klinischer Studien nach den engen Vorgaben des Arzneimittelrechts fand damals noch keine ausführliche Berücksichtigung, da gerade die wissenschaftlich motivierten Arzneimittelstudien noch von dem Regulierungskorsett des AMG ausgenommen waren. Dies hat sich mit der 12. Novelle des AMG 2004 grundlegend geändert. Die vorliegende Neukonzeption einer übergreifenden Forschungsinfrastruktur profitiert somit einerseits von den Erfahrungen einiger Kompetenznetze, die im Gefolge der 12. AMG-Novelle bereits Erfahrungen mit dem Aufbau und der Anpassung ihrer Studieninfra-

strukturen gemäß der Vorgaben des AMG gesammelt haben. Andererseits werden hier Erfahrungen in neuer und generischer Form zusammengefasst, die neuen Forschungsverbünden eine deutlich schnellere und ökonomischere Konzeption, Abstimmung und Umsetzung einer zukunftssicheren und langfristig angelegten Studieninfrastruktur erlaubt. Auch wenn die Vorgaben des AMG für die IT-Unterstützung und Durchführung einzelner Studien berücksichtigt werden, ist die vorgeschlagene Infrastruktur nicht auf diese Form der Forschung festgelegt.

6.4.2 Prozesse und Anwendungsfälle

6.4.2.1 Patienten in das Studienmodul aufnehmen

Der Prozess der Aufnahme von Patienten in eine Studie wurde bereits in Kapitel 5.2 beschrieben. Für die spätere Zusammenführung und Nutzung der Daten aus verschiedenen Studien oder Forschungsprojekten ist allerdings entscheidend, dass die Einwilligungserklärungen zentral hinterlegt oder zumindest ausgewertet werden, da gerade die spätere Nutzung der Daten nur in Übereinstimmung mit einer idealerweise abgestuft formulierten Einwilligungserklärung [5, S. 97] geschehen darf. Zudem ist ein zentrales ID-Management (vgl. Kapitel 6.1) notwendig, welches zumindest die personenbezogene Zusammenführung der Pseudonyme einzelner Studien (Subject Identification Codes, SIC) anhand einer übergeordneten ID (PID_S) erlaubt. Die Patientenliste kann dabei für jede Studie separate IDs (SICs) verwalten und anhand eines einheitlichen Pseudonyms für das Studienmodul (PID_S) einander zuordnen, oder es wird von der Patientenliste für jedes Studien- oder Forschungsprojekt immer das gleiche Pseudonym (PID_S) herausgegeben. Wenn je Studie unabhängige SICs verwendet werden, kann die Patientenliste diese entweder von anderen Softwarekomponenten entgegennehmen und dauerhaft zusammen mit dem PID_S verwalten, oder die Patientenliste erzeugt diese IDs selber und gibt sie auf Anfrage heraus. Diese Prozesse sind bereits ausführlich in Kapitel 5.2 zum Studienmodul als Variante mit zentraler Patientenliste sowie in Kapitel 6.1 beschrieben.

Eine deutliche Vereinfachung und Beschleunigung der Rekrutierung lässt sich erreichen, wenn auf die Daten früherer Forschungsprojekte in einer Forschungsdatenbank in Übereinstimmung mit den entsprechend formulierten Einwilligungserklärungen zurückgegriffen werden kann. Auch hierfür ist ein zentraler Zugriff nicht nur auf die für die Ein- und Ausschlusskriterien relevanten Daten, sondern auch auf die durch die Einwilligungserklärungen festgelegten Nutzungsmöglichkeiten entscheidend. Diese sollten hierfür auch im Forschungsmodul mit hinterlegt sein.

6.4.2.2 Studiendaten erheben, auswerten und archivieren

Die Erhebung, Auswertung und Archivierung der Daten innerhalb einer klinischen Studie oder eines einzelnen Forschungsprojekts richtet sich weitestgehend nach den Anforderungen des konkreten Forschungsvorhabens und ist in Kapitel 5 ausführlicher beschrieben. Die nach Abschluss des Einzelprojekts stattfindende Überführung der Daten in eine übergeordnete Forschungsdatenbank hat auf diese Prozesse keinen direkten Einfluss. Dies gilt auch für Aufgaben wie z.B. das Management unerwarteter Ereignisse samt den damit einhergehenden gesetzlichen Meldeverpflichtungen.

6.4.2.3 Datenqualität im Studienmodul sichern

Ergänzend zu üblichen Qualitätssicherungsverfahren in einzelnen Studien (vgl. Kap. 5.2.2.5) kann bei Kombination mit einem Forschungsmodul auch ein Abgleich von Daten aus verschiedenen Studien zu einem Patienten durchgeführt werden. Eine solche Datenüberprüfung kann durch verschiedene unstimmige Daten ausgelöst werden (vgl. Kap. 6.3.2.3).

Bei der Übermittlung von Kontextdaten aus der Forschungsdatenbank an das zentrale Datenmanagement im Studienmodul zum Zwecke der Qualitätssicherung wird nur eine einstufige Depseudonymisierung benötigt. Diese erste Stufe der Depseudonymisierung sollte als reine Maschinenfunktion angelegt werden, die nur von besonders autorisierten Mitarbeitern des Datenmanagements im Studienmodul angestoßen werden kann. Dieser Anwendungsfall setzt die Definition eines studienübergreifenden Kern- oder Basisdatensatzes voraus, der in jeder Studie erhoben und somit zum Abgleich genutzt werden kann. Die Einwilligung der betroffenen Patienten für den konkret auf diesen Kerndatensatz bezogenen Abgleich mit bereits früher erhobenen Daten muss vorliegen.

Ausgangspunkt des Prozesses ist das zentrale Datenmanagement im Studienmodul, welches für alle Probanden, die bereits an einer vorhergehenden Studie teilgenommen haben, die PID_S sammelt und an den Pseudonymisierungsdienst schickt, der diese symmetrisch in PSN umschlüsselt und an die Forschungsdatenbank weiterreicht. Dort werden die zu den PSN zugehörigen Kerndatensätze herausgesucht und wiederum an den Pseudonymisierungsdienst geschickt, der diese nach symmetrischer Umschlüsselung der PSN in PID_S an das Datenmanagement im Studienmodul ausliefert. Dort können dann automatisierte Auswerteroutinen den Abgleich vornehmen und Auffälligkeiten in den Daten für eine weitere Überprüfung kennzeichnen.

Alternativ kann dieser Prozess auch über einen SIC aus der Studiendatenbank gesteuert werden. Hierfür ist die Einschaltung der Patientenliste über ein Ticket-Handling nötig, so dass der PID_S gegenüber der Studienzentrale nicht offenbart werden muss und andererseits die Patientenliste keinen Zugriff auf medizinische Daten erhält.

6.4.2.4 Datenqualität im Forschungsmodul sichern

Es kann die Notwendigkeit bestehen, medizinische Daten, die sich schon in der Forschungsdatenbank befinden und im Regelfall bereits einen aufwändigen Qualitätssicherungsprozess durchlaufen haben, trotzdem noch einmal zu ändern oder zu korrigieren. Im Zusammenhang mit einem Studienmodul wird dies z.B. dann notwendig, wenn im Rahmen der aktuellen Studie festgestellt wird, dass bereits in einem früheren Forschungsprojekt erhobene Basisdaten eines Patienten aktualisiert werden müssen (vgl. Kap. 5.2.2.5 zur Qualitätssicherung). Ein anderer Fall liegt vor, wenn allein in den Daten der Forschungsdatenbank Inkonsistenzen oder Fehler entdeckt werden, die jedoch nur mit Rückgriff auf die Quelldaten behoben werden können.

Wenn der Aktualisierungsbedarf im zentralen Datenmanagement des Studienmoduls entdeckt wird, übermittelt dieses den aktualisierten Datensatz mit dem zugehörigen PID_S an den Pseudonymisierungsdienst im ID-Management, der die Umschlüsselung des PID_S in ein PSN übernimmt und die Daten dann an die Forschungsdatenbank weiterleitet. Hier wird der Datensatz anhand des Pseudonyms PSN selektiert und geändert bzw. überschrieben.

Werden hingegen Fehler oder unplausible Daten im Forschungsmodul selbst festgestellt und ist ein Rückgriff auf die Quelldaten notwendig, ist ein anderes Vorgehen einzuhalten. Zunächst wird zu dem betreffenden Datensatz das Pseudonym PSN ermittelt und zusammen mit einer Fehlerbeschreibung über den Pseudonymisierungsdienst an die für die identifizierenden Daten zuständige Stelle im ID-Management geschickt. Diese nimmt daraufhin Kontakt mit dem aktuell behandelnden Arzt auf und leitet die Anfrage mit der Fehlerbeschreibung weiter. Nach Beantwortung der Anfrage wird ein ggf. korrigierter Datensatz vom behandelnden Arzt an die zentrale Stelle im ID-Management und von dort mit dem PID_S über den Pseudonymisierungsdienst an das Datenmanagement im Forschungsmodul weitergeleitet. Dort kann anhand des PSN eine Korrektur des betreffenden Datensatzes vorgenommen werden.

Aus Sicht des Datenschutzes kann es dem Betreiber der Forschungsdatenbank überlassen werden, ob er die Änderung in Form einer Versionierung oder mit Hilfe eines Audit Trails nachvollziehbar macht. Im Sinne einer hohen Datenqualität sind aber Funktionen, die eine Nachvollziehbarkeit aller Änderungen gewährleisten, auf jeden Fall zu empfehlen.

6.4.2.5 Daten vom Studienmodul in das Forschungsmodul übermitteln

Auch wenn in die hier konzeptuell beschriebene Forschungsdatenbank Daten aus ganz unterschiedlichen Quellen eingespeist werden können, steht in der folgenden Beschreibung die Übernahme von Daten aus klinischen Studien oder anderen, einzeln über ein Studienmodul abgewickelten Forschungsprojekten im Vordergrund. Dabei werden die Daten üblicherweise nach Abschluss

eines Forschungsprojekts oder zumindest nach Abschluss der Qualitätssicherung in die langfristig angelegte Forschungsdatenbank transferiert. Für diesen Prozess sind folgende Voraussetzungen entscheidend:

- Der Patient hat in die pseudonymisierte Speicherung nach Abschluss des konkreten Forschungsvorhabens eingewilligt.
- Der Patient hat in die Auswertung und Nutzung seiner Daten über die konkrete Fragestellung der aktuellen Studie hinaus eingewilligt.
- Der in die Forschungsdatenbank übertragene medizinische Datensatz erlaubt im Zusammenhang mit ggf. dort bereits gespeicherten Daten weiterhin eine pseudonyme Speicherung, d.h. dass auch bei Nutzung aller medizinischen Daten eines Patienten nach wie vor eine Reidentifizierung faktisch ausgeschlossen bleibt.
- Die Kennung der medizinischen Einrichtungen oder der individuellen Ärzte kann in den Forschungsdaten im Klartext oder ebenfalls pseudonymisiert gespeichert werden. Vor einer Speicherung solcher Daten im Klartext muss geklärt werden, dass hierdurch kein relevantes Reidentifizierungsrisiko entsteht.

Wenn diese Voraussetzungen gegeben sind, müssen die Datensätze mit einem langfristig sicheren Pseudonym versehen werden, welches an keiner weiteren Stelle im Zusammenhang mit den identifizierenden Daten der Patienten gespeichert wird. Dies wird durch eine zweite Stufe der Pseudonymisierung in einem Pseudonymisierungsdienst als Teil des Identitätsmanagements umgesetzt.

Als Ausgangspseudonym kann dabei nicht ein studienspezifisches Pseudonym (SIC) verwendet werden, da dann über die daraus gebildeten Pseudonyme der zweiten Stufe keine Zusammenführung von Daten aus mehreren Studien möglich wäre. Somit müssen für den Schritt der zweiten Pseudonymisierung die medizinischen Daten aus der aktuellen Studiendatenbank und die studienunabhängige ID im Studienmodul (PID_S) aus der Patientenliste im Zusammenhang verarbeitet werden, wobei eine physische Zusammenführung der Daten nach Möglichkeit vermieden werden sollte. Insbesondere dürfen die medizinischen Daten nicht an die Patientenliste geschickt werden, da dies die informationelle Gewaltenteilung in Bezug auf identifizierende und medizinische Daten durchbrechen würde. Die folgenden beiden Lösungen werden vorgeschlagen:

1. Die Studiendatenbank enthält bereits den PID_S als übergeordnete ID oder kann diesen problemlos und in Vereinbarkeit mit dem Datenschutzkonzept bei der Patientenliste mit Hilfe eines SIC abfragen. Dann werden die medizinischen Daten mit dem öffentlichen Schlüssel der Forschungsdatenbank asymmetrisch verschlüsselt und zusammen mit dem PID_S an den Pseudonymisierungsdienst geschickt.
2. In der Studiendatenbank ist nur ein studienspezifischer SIC hinterlegt und die übergreifende ID aus der Patientenliste kann aufgrund der

Datenschutzregeln des Forschungsverbunds auch nicht abgefragt werden, bzw. sollte sie der Studienzentrale mit der aktuellen Studiendatenbank nicht zur Kenntnis gelangen. In diesem Falle übermittelt die Studiendatenbank an die Patientenliste nur den aktuellen SIC und erhält von dieser ein Ticket (TKT) als temporäre ID. Daraufhin schickt die Patientenliste den studienunabhängigen PID_S zusammen mit dem gerade erzeugten Ticket an den Pseudonymisierungsdienst. Gleichzeitig werden die medizinischen Daten (MDAT) aus der Studiendatenbank mit dem öffentlichen Schlüssel der Forschungsdatenbank asymmetrisch verschlüsselt und zusammen mit dem von der Patientenliste übermittelten Ticket im Klartext an den Pseudonymisierungsdienst geschickt. Dieser kann dann die verschlüsselten und damit nicht einsehbaren MDAT über das Ticket dem von der Patientenliste empfangenen PID_S zuordnen und gemeinsam verarbeiten. Das Ticketprinzip ist in Kapitel 6.1 in Abbildung 9 veranschaulicht. Der Datentransfer über den Pseudonymisierungsdienst ist zudem in Kapitel 6.1.3.4 beschrieben.

Die Pseudonymisierung selbst wird durch eine symmetrische Umschlüsselung des PID_S in das weitere Pseudonym PSN umgesetzt. Aus Sicherheitsgründen wird der hierfür genutzte Schlüssel unauslesbar auf einer SmartCard oder einer vergleichbar sicheren Umgebung gespeichert. Die medizinischen Daten werden nach dem Umschlüsselungsprozess in unveränderter Form zusammen mit dem PSN an die Forschungsdatenbank im Forschungsmodul übergeben. In der Forschungsdatenbank können die medizinischen Daten (MDAT) anhand des privaten Schlüssels entschlüsselt und mit dem PSN als Ordnungskriterium gespeichert werden.

6.4.2.6 Daten an Forscher weitergeben

Die bei Exporten zu berücksichtigenden Rahmenbedingungen und Prozesse sind bereits in Kapitel 5.3 für isoliert aufgebaute Forschungsdatenbanken beschrieben.

6.4.2.7 Machbarkeit einer Studie prüfen

Um die Machbarkeit einer Studie prüfen zu können, müssen Indizien dazu ausgewertet werden, wie viele den spezifizierten Ein- und Ausschlusskriterien entsprechende Patienten innerhalb einer bestimmten Zeitspanne zu erwarten sind und ggf. in die Teilnahme einer Studie einwilligen würden. Die Daten des hier beschriebenen Forschungsmoduls können hierfür herangezogen werden. Im Regelfall wird für eine solche Analyse kein vollständiger Export von Datensätzen benötigt, sondern es reicht die Herausgabe der Anzahl von Datensätzen innerhalb eines festgelegten Zeitraums, die den spezifizierten Kriterien entsprechen. Das nähere Verfahren ist im Kapitel 5.3 über das Forschungsmodul beschrieben.

6.4.2.8 Rekrutierung unterstützen

Patienten, die bereits an einem früheren Forschungsprojekt teilgenommen haben, können mit Hilfe des Forschungsmoduls auch effektiv für weitere Studien rekrutiert werden, sofern dies durch die Einwilligungserklärung abgedeckt ist. Dies kann insbesondere bei chronischen Erkrankungen von Interesse sein. Anders als bei der Überprüfung der Machbarkeit wird hierfür eine Depseudonymisierung der Datensätze ausgelöst werden müssen, die den gesuchten Ein- und Ausschlusskriterien entsprechen. Idealerweise sollten die hinterlegten Einwilligungserklärungen der ausgewählten Patienten eine direkte Ansprache aus dem Forschungsverbund heraus erlauben. Anderenfalls könnte auch eine Ansprache über die aktuell oder zuletzt behandelnde Einrichtung geregelt sein.

Der Prozess startet im zentralen Datenmanagement des Studienmoduls, wo die Ein- und Ausschlusskriterien zusammengetragen und mit den Metadaten zur Forschungsdatenbank abgeglichen werden. Die aus diesem Abgleich entstandene Abfrage wird vom Ausschuss Datenschutz geprüft und an das Datenmanagement des Forschungsmoduls weitergereicht. Dort werden die PSN der zu dieser Abfrage passenden Datensätze extrahiert und über den Pseudonymisierungsdienst, der eine Umschlüsselung der PSN in die PID_S vornimmt, an das zentrale Datenmanagement des Studienmoduls geschickt. Das zentrale Datenmanagement richtet nun an die für die Speicherung der Identitätsdaten verantwortliche Stelle im ID-Management (z.B. als Treuhänder) die Anfrage, die aktuellen Behandler und ggf. weitere Adressdaten zu den übermittelten PID_S herauszugeben. Die hierfür verantwortliche Stelle prüft die Anfrage und informiert nach Freigabe durch den Ausschuss Datenschutz die aktuellen Behandler über die für eine Rekrutierung in Frage kommenden Patienten. Für den Fall, dass Patienten nicht mehr über den aktuell verzeichneten Behandler angesprochen werden können, sollte eine Alternativlösung vorbereitet werden. In so einem Falle könnte ein Treuhänder beispielsweise die Patienten anhand der Adressdaten direkt ansprechen, siehe auch die Ausführungen zum Kontaktmanagement in den Kapiteln 6.1, 6.5.2.4 (Unterkapitel zu Kontaktdaten) und 6.6.6.

6.4.2.9 Auskunft geben

Wenn ein Patient Auskunft verlangt, welche Daten über ihn gespeichert sind, ist im Falle eines kombinierten Studien- und Forschungsmoduls nicht nur der Datensatz in einer ggf. aktuell laufenden Studie zu berücksichtigen, sondern darüber hinaus eventuell auch im Forschungsmodul gespeicherte Datensätze aus früheren Forschungsprojekten.

Der Patient wendet sich hierzu entweder an seinen behandelnden Arzt oder direkt an eine zentrale, hierfür benannte Stelle des Forschungsverbunds. Diese Stelle kann bei einem zentralen Datentreuhänder angesiedelt sein. Die vom

behandelnden Arzt oder Patienten direkt angefragte Stelle ermittelt den zum Patienten zugehörigen PID_S und übermittelt diesen via Pseudonymisierungsdienst an das Datenmanagement im Forschungsmodul. Zu dem hier ankommenden PSN werden alle zugehörigen Datensätze ermittelt und über den Pseudonymisierungsdienst an die anfragende Stelle zurückgeschickt. Diese reicht die Daten entweder an den Patienten direkt oder an den behandelnden Arzt weiter.

6.4.2.10 Daten im Forschungsmodul umpseudonymisieren

Der Austausch der Pseudonyme einer Forschungsdatenbank kann aus unterschiedlichen Gründen notwendig werden: Z.B. bei Verlust oder Kompromittierung einer zur Pseudonymisierung genutzten SmartCard oder bei drohender Kompromittierung des verwendeten Verschlüsselungsalgorithmus. Liegt die Notwendigkeit eines Austausches der Pseudonyme vor, so muss dieser durch das Identitätsmanagement durchgeführt werden. Hierbei muss durch geeignete Verfahren sichergestellt werden, dass die neuen Pseudonyme dem richtigen Patienten bzw. Datensatz zugewiesen werden.

Das Identitätsmanagement im Forschungsverbund teilt dem Forschungsmodul mit, dass eine Umpseudonymisierung nötig ist. Das Forschungsmodul ermittelt dann alle betroffenen Pseudonyme PSN, ggf. auch aus mehreren Forschungsdatenbanken, und schickt diese an den Pseudonymisierungsdienst im Identitätsmanagement. Dieser transformiert die PSN zunächst mit Hilfe der bisherigen Smartcard zurück in den studienübergreifenden PID_S und im Anschluss mit Einsatz der neuen Smartcard in ein neues Pseudonym. Für diesen Prozess muss das Forschungsmodul die neuen PSNs eindeutig den Datensätzen korrekt zuordnen können, die bisher mit den alten PSNs markiert waren.

6.4.2.11 Daten sperren, anonymisieren oder löschen

Wenn keine Notwendigkeit für die Speicherung pseudonymisierter Daten im Forschungsmodul besteht, sind diese zu löschen oder zu anonymisieren. Wenn eine Anonymisierung möglich ist, wird dieser im Sinne weiterer wissenschaftlicher Verwertung der Daten vor dem Löschen der Vorzug zu geben sein. Auslöser der Anonymisierung können der Wunsch des Patienten, dessen Versterben oder das Verstreichen einer spezifizierten Frist seit der letzten Studienteilnahme sein. In letzterem Falle ist die Frist so zu bemessen, dass nach Ablauf der Frist eine erneute Teilnahme des Patienten an einer Studie im gleichen Forschungsverbund und damit die Erhebung von Follow-up-Daten so unwahrscheinlich ist, dass die weitere Speicherung pseudonymisierter Daten nicht mehr gerechtfertigt erscheint. Die hierfür relevante Frist ist im Datenschutzkonzept des Forschungsverbunds festzulegen und der Patient darüber zu informieren.

Die Anonymisierung wird vom ID-Management des Forschungsverbunds aus gesteuert, welches entweder bei Verstreichen der festgelegten Frist ohne Follow-ups diese selbst initiiert oder von einer behandelnden Einrichtung oder aus dem Umfeld des Patienten über einen Widerruf oder das Versterben des Patienten informiert wird.

In der Patientenliste des ID-Managements wird dann das studienübergreifende Pseudonym PID_S ermittelt und mit der Anonymisierungsanfrage über den Pseudonymisierungsdienst an das Forschungsmodul übermittelt. Der Pseudonymisierungsdienst ersetzt in dieser Anfrage den PID_S durch das symmetrisch verschlüsselte Pseudonym PSN und schickt die Anfrage an das Forschungsmodul weiter.

Im Forschungsmodul muss in jedem Fall sichergestellt sein, dass die Daten in allen beteiligten Forschungsdatenbanken anonymisiert werden. Es ist, z.B. durch die Wahl eines geeigneten Präfixes oder Suffixes, darauf zu achten, dass die anonymen IDs nicht mit pseudonymisierten IDs zu verwechseln sind. Wenn nur wenige Datensätze mit anonymen IDs versehen sind, muss ggf. zur Verhinderung einer Reidentifizierung auf eine eindeutige Markierung anonymer IDs verzichtet werden. Die Anonymisierung kann im Einzelfall und nach Abschätzung des Reidentifizierungsrisikos auch erfordern, dass einzelne charakteristische Merkmale des Falls gelöscht oder vergröbert werden.

Nach der Anonymisierung der Daten im Forschungsmodul muss die Löschung der identifizierenden Daten in der Patientenliste im Identitätsmanagement veranlasst werden. Ggf. sind auch Patientenlisten in den behandelnden Einrichtungen zu löschen.

Wenn das Löschen von Datensätzen im Forschungsmodul erforderlich ist, wird auch dieser Prozess von der Patientenliste im ID-Management gesteuert. Hierzu wird ebenfalls der studienübergreifende PID_S ermittelt und über den Pseudonymisierungsdienst mit der Löschungsaufforderung an das Forschungsmodul geschickt. Im Forschungsmodul werden dann in allen beteiligten Forschungsdatenbanken alle Datensätze mit dem zum PID_S korrespondierenden PSN gelöscht. Im Anschluss sind die IDAT in der Patientenliste und ggf. in den beteiligten Zentren lokal gespeicherte Zuordnungslisten zu löschen.

6.4.3 Nutzer, Rollen und Rechte

Neben der Patientenliste wird für das ID-Management bei Verknüpfung eines Studienmoduls mit einem Forschungsmodul auch ein Pseudonymisierungsdienst benötigt. Somit muss für das ID-Management nicht nur das Personal für die Administration der Patientenliste (s. Kap. 5.2.4) betrachtet werden sondern zusätzlich auch jenes für den Pseudonymisierungsdienst. Die Administration der beiden Dienste im ID-Management sollte unter getrennter Verantwortung stehen, so dass auch getrenntes Personal benötigt wird. Für den

Pseudonymisierungsdienst sollte eine administrative Kraft vorgesehen werden, die vollen Zugriff auf die Software, Einstellungen und das Handling der Smartcards hat. Das Personal im ID-Management wird, von administrativen Ausnahmen abgesehen, vor allem auf Anweisungen des Ausschusses Datenschutz tätig und wird entsprechend den Vorgaben die einfache oder vollständige Depseudonymisierung unterstützen.

Für das Studienmodul mit seinen Studiendatenbanken und behandelnden Einrichtungen sind im vorliegenden Verknüpfungsszenario die gleichen Nutzer und Rollen vorzusehen, wie sie bereits in Kapitel 5.2.4 beschrieben wurden. Insbesondere sind die Studienärzte und unterstützende Kräfte in den beteiligten Zentren, administratives Personal je Studiendatenbank, Monitore und ggf. Personal eines kommerziellen oder universitären Sponsors als Nutzer mit entsprechenden Rechten einzurichten.

Wie im Falle eines einfachen Studienmoduls muss auch geklärt werden, ob Patienten selbst in die Dokumentationsprozesse eingebunden werden. Entsprechend sind die Voraussetzungen hierfür zu schaffen (vgl. Kap. 5.2.4).

Der Zugriff auf eine oder mehrere Datenbanken im Forschungsmodul kann durch den Administrator sowie autorisierte Forscher erfolgen. Der Administrator hat vollen Zugriff auf die Datenbanken und kann entsprechende Selektionen und Exporte veranlassen. Der Forscher kann seinem Antrag entsprechend bestimmte Teile der Forschungsdatenbank einsehen. Während der Administrator die PSN im Forschungsmodul sehen darf, bleiben diese dem Forscher verborgen. Im Falle mehrerer Datenbanken im Forschungsmodul kann es auch getrennte administrative Zuständigkeiten für die einzelnen Datenbanken geben. Dabei muss aber eine einheitliche Schnittstelle zum Pseudonymisierungsdienst des ID-Managements gewährleistet bleiben.

6.4.4 Verantwortlichkeiten

Die Gesamtverantwortung liegt beim Forschungsverbund, was durch eine passende Rechtsform auch einen rechtsverbindlichen Ausdruck bekommt. Der Forschungsverbund beauftragt unterschiedliche Stellen mit den Aufgaben des ID-Managements sowie der Führung des Studien- und Forschungsmoduls. Dabei ist die Aufsicht über die beiden Komponenten Patientenliste und Pseudonymisierungsdienst des ID-Managements an zwei separate und voneinander unabhängige Institutionen zu vergeben. Ebenfalls unabhängig voneinander sollte die Aufsicht über das Studien- und das Forschungsmodul organisiert werden. In begründeten Einzelfällen kann von dieser Form der vollständigen informationellen Gewaltenteilung abgewichen werden. Die hierfür relevanten Entscheidungskriterien werden in Kapitel 6.7 dargestellt und diskutiert.

Die Verantwortlichkeiten innerhalb des Studienmoduls sind grundsätzlich so wie in Kapitel 5.2.5 beschrieben zu regeln. Im vorliegenden Falle ist lediglich

die Einbettung in die beim Forschungsverbund liegende Gesamtverantwortung zu berücksichtigen. Dies gilt auch für die Regelung der Verantwortlichkeiten in den beteiligten Zentren bzw. den behandelnden Einrichtungen. Diese und die Verantwortlichkeiten in der Studienzentrale müssen im Falle gesetzlich geregelter Studien nach AMG oder MPG zudem auch den gesetzlichen Anforderungen genügen. Eine übergeordnete Verantwortlichkeit kommt dann dem Sponsor der Studie zu. Wenn Prozesse, wie z.B. die Archivierung der Daten, ausgelagert werden, ist eine klare Delegationsregelung erforderlich.

Die Einrichtung eines „Ausschusses Datenschutz" als zentrales Gremium für die Beratung und Entscheidung datenschutzrechtlich sensibler Fragen wird dringend empfohlen. Dieses Gremium ist zudem für die Vorgabe von Richtlinien und Policies im Umgang mit den Daten zuständig.

Die Patientenliste ist der sensibelste Teil des Identitäts-Managements und hat damit, wenn sie zentral geführt wird, einen hohen Schutzbedarf. Datenschutzrechtlich ist zu berücksichtigen, dass die IDAT, obwohl sie in der Patientenliste nicht mit medizinischen Daten (MDAT) kombiniert werden, den betroffenen Personenkreis ggf. als Patienten eines Forschungsnetzes mit einem umschriebenen Krankheitsspektrum ausweisen. Im Falle eines stigmatisierenden oder in anderer Hinsicht sensiblen Krankheitsbereichs ist daher eine auch in den Augen der betroffenen Patienten besonders vertrauenswürdige Stelle mit der Führung der Patientenliste zu beauftragen.

Der Zugriff auf die Daten der Forschungsdatenbank kann nur nach Bewilligung durch den Ausschuss Datenschutz gewährt werden. Dabei werden der Forschungsansatz und der dafür benötigte Datensatz geprüft. Das Gremium leitet die Bewilligung an den Administrator des Forschungsmoduls weiter, der die Daten entsprechend der genehmigten Anforderung des Wissenschaftlers selektiert und exportiert oder ggf. dem Forscher eine selektive Sicht auf die Forschungsdatenbank ermöglicht.

6.4.5 Aspekte der Realisierung

Zentral für die Verzahnung eines Studienmoduls mit einem Forschungsmodul ist ein auslagerbarer Pseudonymisierungsdienst, der eine sichere Trennung der einstufig und zweistufig pseudonymisierten Datenbestände ermöglicht. Dieser Pseudonymisierungsdienst darf als Komponente des ID-Managements lediglich Zugriff auf die Pseudonyme selbst und nicht etwa auf MDAT oder IDAT haben. Da die MDAT zwischen den Systemen „vor" und „hinter" dem Pseudonymisierungsdienst transferiert werden müssen, ist für diese ein asymmetrisches Verschlüsselungsverfahren zu nutzen, bei dem der Absender jeweils den öffentlichen Schlüssel des Empfängers zum Verschlüsseln verwendet. So kann sichergestellt werden, dass nur die empfangende Komponente mit ihrem privaten Schlüssel die MDAT entschlüsseln und lesen kann. Alternativ zu diesem Ansatz ist auch ein Ticketsystem möglich, bei dem die MDAT

gar nicht an den Pseudonymisierungsdienst geschickt werden, sondern mit Hilfe eines temporären Tickets direkt vom Sender zum Empfänger geschickt werden können. Beide alternativen Möglichkeiten sind in Abbildung 9 veranschaulicht.

Der erste Weg, der eine asymmetrische Verschlüsselung nutzt, wird bereits in der aktuellen Version des Pseudonymisierungsdienstes der TMF (PSD) unterstützt. Dieser Dienst besteht aus drei Softwarekomponenten, die die gesamte Kommunikation abbilden. Die erste Komponente wird im Sicherheitskontext der zentralen Datenbank des Studienmoduls installiert und nimmt dort unverschlüsselte MDAT und einen PID_S in einer vordefinierten XML-Struktur entgegen. Diese XML-Struktur besteht aus einem vordefinierten Header, der u.a. den Absender und den umzuschlüsselnden PID_S enthält. In dem nicht weiter vordefinierten und frei nutzbaren Body-Teil der XML-Struktur können die MDAT in unverschlüsselter Form hinterlegt werden. Diese Softwarekomponente des PSD sorgt für eine asymmetrische Verschlüsselung der MDAT und schickt dann die XML-Struktur an die zentrale Komponente des PSD, wo mit Hilfe eines auf einer Smartcard sicher gehaltenen Schlüssels eine symmetrische Umschlüsselung des PID_S in das langfristig nutzbare Pseudonym PSN erfolgt. Mit diesem PSN im Header der XML-Struktur werden die Daten dann an die dritte Komponente weiter geleitet, die im Sicherheitskontext des Forschungsmoduls installiert ist. Diese Komponente kann mit dem dort verfügbaren privaten Schlüssel des Forschungsmoduls die MDAT entschlüsseln und zusammen mit dem PSN der Datenbank des Forschungsmoduls zur Verfügung stellen.

Diese Lösung kann auch genutzt werden, um Daten verschiedenen Datenbanken im Forschungsmodul zur Verfügung zu stellen, wobei die Adressierung für den PSD transparent im Sinne von unsichtbar erfolgt, d.h. diese wird innerhalb der MDAT vorgenommen. So können z.B. Bilddaten in eine separate Bilddatenbank transferiert werden, während die klinischen Verlaufsdaten in einem anderen Datenbanksystem landen.

Zusätzlich verfügt der PSD über einen Finding-Manager, der die Möglichkeit bietet, einen im Forschungsmodul ermittelten relevanten Befund auf sicherem Wege zum behandelnden Arzt zu übermitteln. Für die Aufrechterhaltung einer langfristigen Sicherheit der Pseudonyme im Forschungsmodul verfügt der PSD zudem über die Funktion eines Recryptings aller PSN mit Hilfe der alten und einer neuen Smartcard mit neuem Schlüssel.

Eine Erweiterung des PSD ist dahingehend geplant, dass auch ein Ticketsystem zum direkten Transfer der MDAT zwischen den Komponenten in Studien- und Forschungsmodul unterstützt wird. Ebenso eine Erweiterung um die Funktion einer Vermittlung eines SIC in einen PID_S mit Hilfe einer Kommunikation mit der zentralen Patientenliste des ID-Managements.

6.5 Das Maximalmodell eines medizinischen Forschungsverbundes

6.5.1 Zweck und Anwendungsbereich

Dieses Kapitel beschreibt einen Forschungsverbund, in dem ein ganzes Spektrum medizinischer Forschung zu einem bestimmten Krankheitsbild oder zu einer Gruppe zusammengehöriger Krankheitsbilder – von der molekulargenetischen über die klinische (beobachtende und interventionelle) bis zur epidemiologischen Forschung – in Kooperation organisiert wird. Weiterhin wird angenommen, dass im Forschungsverbund die Notwendigkeit zu langfristiger Aufbewahrung von Daten und Proben besteht und es größere Patienten- und Probandenzahlen gibt, es sich also nicht z.B. um eine seltene Erkrankung handelt (s. hierzu auch unter „Verhältnismäßigkeit", Kap. 6.7).

Ein medizinischer Forschungsverbund im Maximalmodell benötigt jedes der Module

- Klinisches Modul,
- Studienmodul,
- Forschungsmodul und
- Biobankenmodul

sowie dazu als zentrale Infrastruktur u.a. die Komponenten

- Identitätsmanagement und
- Rechtemanagement.

Diese Struktur ist in Abbildung 8 dargestellt.

In jedem der Module können unter Umständen auch mehrere Datenbanken gleicher Art angesiedelt sein; insbesondere im Studienmodul ist es oft nicht sinnvoll oder machbar, eine gemeinsame zentrale Datenbank für alle im Forschungsverbund durchgeführten klinischen Studien einzurichten.

Werden im Forschungsverbund auch in größerem Umfang Bilddaten erzeugt und aufbewahrt, sind als Komponenten eine oder auch mehrere eigenständige Bilddatenbanken vorzusehen; diese werden in einem eigenen Modul angesiedelt oder – bei entsprechend eingeschränktem Verwendungszweck – in Klinisches, Studien- oder Forschungsmodul integriert. Auch innerhalb eines solchen Moduls ist bei entsprechender Einschätzung des Reidentifizierungsrisikos unter Umständen die Speicherung von Bildern in einer auch für Daten genutzten, bereits vorhandenen Datenbank möglich oder in einer getrennten Datenbank notwendig. Eine organisatorisch getrennte Speicherung von Bilddaten ist dann nötig, wenn diese – z.B. als Fotografien des Gesichts – die Person leicht erkennen lassen. Kriterien für die einzelnen Optionen werden im Kapitel zur Verhältnismäßigkeit aufgeführt.

6.5.2 Prozesse und Anwendungsfälle

Die für das Maximalmodell relevanten Prozesse umfassen die Gesamtheit der bei den einzelnen Modulen und bei deren Zusammenspiel behandelten Prozesse. Hier wird zunächst für das Maximalmodell der typische Weg eines Patienten durch die Module des Forschungsverbunds beschrieben, danach folgen einige für das Maximalmodell nötige Erweiterungen und Ergänzungen zu den bereits in früheren Kapiteln beschriebenen Prozessen.

6.5.2.1 Patienten aufnehmen

Patienten werden im Maximalmodell bevorzugt in das Klinische Modul aufgenommen und in dessen Rahmen behandelt; ihre Daten werden in einer Klinischen Datenbank gespeichert, die auch als Grundlage für Beobachtungsstudien dient, wie in Kapitel 5.1 beschrieben. Der Forschungsverbund führt auch klinische Studien im Sinne des AMG oder MPG durch; dieses wird in Kapitel 5.2 beschrieben. Für diese Studien können geeignete Patienten aus dem Klinischen Modul, unter Umständen auch aus dem Forschungsmodul oder der Biomaterialbank gewonnen werden. Die Gewinnung von Teilnehmern an neuen Studien ist beispielsweise in Kapitel 5.3.2.5 für eine Forschungsdatenbank beschrieben. Da es sich dabei um Interventionsstudien handelt, muss für die Teilnahme eine neue gesonderte Einwilligungserklärung eingeholt werden; dies ist mit vertretbarem Aufwand möglich, da der Betroffene ja ohnehin kontaktiert werden muss. Hierfür werden die ADAT (s. Kap. 6.5.2.4) benötigt.

Auch nach Aufnahme in das Studienmodul verbleibt ein Patient in der Regel weiterhin im Klinischen Modul; das Zusammenspiel der beiden Module ist in Kapitel 6.3 beschrieben. Patienten, die direkt (primär) als Studienteilnehmer gewonnen wurden, werden, in Abhängigkeit von den Erfordernissen des Forschungsverbunds und der Einwilligung, parallel dazu auch in das Klinische Modul aufgenommen.

Gesunde Probanden, die als Kontrollpersonen am Forschungsmodul teilnehmen, können auch direkt dort aufgenommen werden.

Proben des Patienten oder Probanden werden an das Biobankenmodul übergeben und dort wie in Kapitel 5.4 beschrieben behandelt. Spätestens wenn der Patient nach den in Kapitel 5.1 formulierten Kriterien nicht mehr im Klinischen Modul geführt werden soll oder darf und auch an keiner klinischen Studie des Forschungsverbunds mehr teilnimmt, werden die Daten in das Forschungsmodul überführt, das in Kapitel 5.3 beschrieben wurde; der Übergang vom Studien- in das Forschungsmodul wird in Kapitel 6.4 behandelt. Im Forschungsmodul werden die Daten – abhängig natürlich von der vorliegenden Einwilligung – ebenso wie die Proben und Analyseergebnisse im Biobankenmodul in der Regel langfristig aufbewahrt.

6.5.2.2 Erweiterte Prozessbeschreibungen

Prozesse, die im Maximalmodell mehrere oder alle Module betreffen, sind der Widerruf, der Todesfall und die Qualitätssicherung. Die nötigen Erweiterungen sind:

- **Widerruf**: Widerruft ein Patient oder Proband seine Teilnahme am gesamten Forschungsverbund, so muss – in Abhängigkeit von den Regelungen der Einwilligungserklärung – dafür gesorgt werden, dass seine Daten in allen Modulen des Verbundes gelöscht bzw. anonymisiert werden. Für die Anonymisierung bedeutet dies insbesondere, dass alle noch im Klinischen oder Studienmodul befindlichen Daten in das Forschungsmodul übertragen und die IDAT im Identitätsmanagement gelöscht werden. Hierbei ist in jedem Einzelfall darauf zu achten, dass durch diese Datenzusammenführung kein erhöhtes Reidentifizierungsrisiko entsteht.
- **Todesfall**: Im Todesfall werden, sobald die Datenerhebung zum Fall abgeschlossen ist, die Daten und Proben in allen Modulen des Forschungsverbundes anonymisiert wie im Fall „Widerruf" beschrieben. Anderweitige Vereinbarungen aus der Einwilligungserklärung sind zu berücksichtigen.
- **Qualitätssicherung**: Ergeben sich bei Qualitätssicherungsmaßnahmen in einem Modul Datenänderungen (in der Regel sind das Fehlerkorrekturen), so sind diese den anderen Modulen mitzuteilen, sofern sie dort relevant sind. Für die richtige Zuordnung der pseudonymen Daten ist die Mitwirkung des Identitätsmanagements notwendig (s.a. Kap. 6.8).

Ein Prozess, der im Maximalmodell neu auftritt, betrifft einen Patienten, der an einer klinischen Studie teilnimmt und sowohl in einer Klinischen als auch in einer Studiendatenbank des Forschungsverbunds geführt wird, wenn seine Daten in die Forschungsdatenbank übermittelt werden (*simultane Übermittlung an die FDB*). In dieser Situation ist der Prüfarzt der Studie im Sinne des Studienmoduls in aller Regel gleichzeitig behandelnder Arzt im Sinne des Klinischen Moduls. Hierzu ist nach Möglichkeit die Anwendungssoftware so zu gestalten, dass diese beiden Übermittlungsvorgänge durch eine einzige Aktion gemeinsam gestartet werden; entsprechende Anforderungen wurden in Kapitel 6.1.6.2 formuliert.

6.5.2.3 Bilddaten

Bilddaten können zu verschiedenen Zwecken in einem Forschungsverbund wichtig sein:

- Im Klinischen Modul oder Studienmodul werden Bilder zur Referenzdiagnostik benötigt; hier besteht in der Regel ein Behandlungszusammenhang im Sinne einer konsiliarischen Tätigkeit, da das Ergebnis der Referenzbefundung direkten Einfluss auf die Behandlung des Patienten hat.

- Zur Verbesserung der Versorgung – nicht des abgebildeten Patienten, sondern weiterer Patienten mit ähnlichem Krankheitsbild – dient die Bereitstellung von Bildern als Vergleichsmaterial für den diagnostischen Prozess.
- Ferner können Bilder zu Ausbildungszwecken als Anschauungsmaterial bereitgestellt werden.
- Und schließlich können Bilddaten wie alle anderen Daten zu Auswertungen im Forschungszusammenhang dienen.

Für die Erhebung und Bereitstellung von Bilddaten im Forschungsverbund gilt das allgemeine Ablaufmodell für medizinische Daten mit nur geringfügigen Modifikationen. Folgende Besonderheiten müssen beachtet werden:

Generell enthalten vor allem Schichtbilddaten Informationen, aus denen mit Hilfe moderner dreidimensionaler Rekonstruktionsverfahren morphologische Informationen über einen Patienten rekonstruiert werden können; so kann z.B. das Gesicht einer Person aus einer Computertomographie des Schädels erzeugt werden. Dies birgt die Gefahr, dass trotz Anonymisierung oder Pseudonymisierung und der Löschung der identifizierenden Daten aus dem DICOM-Header[35] die Möglichkeit besteht, solche Rekonstruktionen mit biometrischen Daten aus anderen Quellen abzugleichen und so den Patienten zu identifizieren. Eine solche Rekonstruktion ist aber – zumindest zurzeit noch – mit einem sehr hohen Aufwand verbunden; die Risiko-Einschätzung ähnelt also der für genetische Daten: Man kann mittelfristig nicht von einer wirksamen Anonymisierbarkeit ausgehen. Eine Speicherung und Verwendung der Daten, soweit sie für die Zwecke des Forschungsverbunds unverzichtbar sind und der Forschungsverbund hierfür verbindliche Regelungen getroffen hat, ist in pseudonymisierter Form mit der entsprechenden Einwilligung langfristig möglich.

Eine weitere Besonderheit betrifft das so genannte Einbrennen von Patienten identifizierenden Daten in das Bildmaterial selbst. Solche Daten finden sich vor allem auf gescannten Röntgenbildern oder auch in Datensätzen aus Ultraschallgeräten. Hier ist ein nachträgliches Löschen der Daten, z.B. durch eine (semi-)automatisierte „Schwärzung" der betroffenen Bereiche, erforderlich. Da dieser Vorgang zum Teil sehr kompliziert, in bestimmten Datenformaten sogar kaum zu lösen ist, muss bereits im Vorfeld einer Studie geklärt werden, welche Geräte für die Datenerhebung eingesetzt werden sollen, um ihre spezifischen Eigenschaften prüfen und entsprechende Löschprozeduren implementieren zu können. Alternativ muss das Einbrennen der Daten von vornherein verhindert werden.

Bilder, insbesondere Fotografien von Gesichtszügen oder besonderen persönlichen Merkmalen, auf denen der Patient leicht zu erkennen oder wieder zu

35 Für die technische Ausführung des Löschvorgangs sei auf das Datenschutzkonzept „TMI-Server" verwiesen. Dieses kann bei der Geschäftsstelle der TMF angefragt werden (www.tmf-ev.de/datenschutz).

erkennen ist und bei denen die Erkennbarkeit nicht zu entfernen ist, sollten in der Einwilligung explizit erwähnt und besonders restriktiv gehandhabt werden. Um die Reidentifizierung der zugehörigen klinischen Daten zu verhindern, ist hier insbesondere eine getrennte Speicherung und ein separates Pseudonymisierungsschema (pseudonymer PID_B) vorzusehen.

Die so aufbereiteten Bilder werden – nach einem evtl. nötigen zusätzlichen Qualitätssicherungsprozess – in eine Bild-Datenbank oder, wie in Kapitel 6.5.1 beschrieben, eine andere Datenbank des Forschungsverbunds übertragen.

6.5.2.4 Organisatorische Daten

Organisatorische Daten (OrgDAT) gehören zu einer höheren Abstraktionsstufe (bzw. einer niedrigeren Prozessschicht) des IT-Modells. Ihre Notwendigkeit und ihr Informationsgehalt ergeben sich aus den Anforderungen der Datenprozessierung im Netz, sie sind nicht von vornherein durch die fachlichen Anforderungen des Forschungsverbunds definiert, so wie etwa IDAT und MDAT. Daher sind sie sehr von der konkreten Implementation der Prozesse im Forschungsverbund abhängig; generisch können nur einige allgemeine Aussagen gemacht werden.

OrgDAT begleiten andere Datenarten (z.B. MDAT in verschiedenen Kontexten) als eine Art von Metadaten und erfüllen folgende Zwecke:

Zugriffsregelung

OrgDAT dienen z.T. der Zugriffsregelung, vor allem im Klinischen Modul, u.U. auch im Studienmodul. Dann ist ihr *logischer* Platz im Rechtemanagement, z.T. auch im Identitätsmanagement. So enthält die Patientenliste auch die Information, wer als behandelnder Arzt (ADAT) für einen Patienten beim Forschungsnetz erfasst ist und damit Zugriffsberechtigung auf die Daten eines Patienten im Klinischen Modul hat; im Studienmodul kann das analog geregelt werden, sofern dort nicht die Zugriffe ohnehin innerhalb der Studiensoftware zufrieden stellend abgesichert werden können. Diese ADAT sind daher zusammen mit den IDAT zu speichern, das heißt, die behandelnden Ärzte sind den Patienten zugeordnet. Die Arztdaten können auch aus einem (pseudonymen) Verweis auf eine separat geführte Arztdatenbank bestehen. Die Informationen zur Zugriffsberechtigung auf einzelne Patientendatensätze befinden sich also auf dem Server der Patientenliste. Zu den OrgDAT gehören auch Zugriffstickets, die aber nur temporär sind und daher nicht mit anderen Daten permanent gespeichert werden.

Kontaktdaten

Bei der Anmeldung eines Patienten bei der Patientenliste werden das Kennzeichen der meldenden Klinik und das Datum der Meldung übertragen und in

der Liste gespeichert (als Teil des ADAT-Satzes). Dies gilt auch dann, wenn einem Patienten bereits ein PID zugewiesen wurde und dieser einer neu meldenden Klinik übermittelt wird. Kennzeichen und Datum werden nicht als Historie geführt, sondern durch die jeweils aktuelle Meldung überschrieben. Die Daten werden benötigt, damit die Stelle, welche die Patientenliste führt, erkennen kann, welche Klinik oder welcher Arzt informiert werden muss, wenn ein Patient in einem der dafür vorgesehenen Anwendungsfälle depseudonymisiert wird.

Dokumentation des Patientenwillens

Zu MDAT (in welchem Modul auch immer) sowie zu Proben und daraus gewonnenen AnaDAT gehören OrgDAT mit den Informationen, was im Rahmen der Patienteneinwilligung mit den zugehörigen Nutzdaten oder Proben gemacht werden darf. Hierzu gehören auch Kontaktinformationen, also in der Regel ein Verweis auf den behandelnden Arzt (ADAT). Um dadurch nicht einen erleichterten Abgleich bei unbefugter Kenntnisnahme von IDAT und MDAT zu ermöglichen, sollen die ADAT allerdings nicht an mehreren unabhängigen Stellen mitgeführt werden; in der Regel ist die Patientenliste der geeignete Speicherort für die ADAT, während die direkten Angaben zur Regelung in der Patienteneinwilligung mit den MDAT bzw. AnaDAT zusammen gespeichert werden.

Prozessunterstützung

Hier fallen OrgDAT etwa als Auftragsbeschreibungen bei der Kommunikation (z.B. Befundanforderung und Rückmeldung) an: Auftraggeber und Adressat, Umfang des Auftrags, Datum, Fristen, Besonderheiten. OrgDAT benötigt man auch zur Definition des Status der zugehörigen Daten oder Proben (z.B. für Qualitätssicherung und Monitoring oder, bei Proben, als Hinweise auf Aliquots).

Qualitätssicherungsaspekte können es erforderlich machen, die Daten vor ihrer Überführung in die Forschungsdatenbank, d.h. vor der zweiten Stufe der Pseudonymisierung, zu prüfen (s. 6.8). In diesem Fall wird eine temporäre Datenbank TempDB eingerichtet. In dieser werden die Daten: PID, MDAT, OrgDAT, $LabID_{tr}$ zusammen mit dafür nötigen OrgDAT kurzzeitig gespeichert. Hier können sie in einem definierten kurzfristigen Zeitraum zur Qualitätssicherung genutzt werden. Bei der Pseudonymisierung und Übertragung in die Forschungsdatenbank werden die Daten in der TempDB gelöscht.

OrgDAT werden in größerem Umfang im Biobankenmodul benötigt. Hier sind sie Begleitdaten einer Probe, die an unterschiedlichen Stellen entstehen und verwendet werden. So erfasst z.B. die Proben gewinnende Stelle die Probenart und gegebenenfalls die Informationen zu Probenentnahme und Präanalytik.

In der Probenbank werden die Begleitdaten einer Probe mit weiteren Informationen wie z.B. den Umständen von Konservierung, Lagerung und Qualität gespeichert. Für weitere Details sei auf das Datenschutzkonzept für Biomaterialbanken [2] verwiesen.

Auch in „angehefteten Dokumenten“ können OrgDAT enthalten sein, z.B. in eingescannten Formularen oder in Röntgenbildern. Hier ist auf den Gehalt solcher Dokumente an identifizierenden Daten zu achten. (Z.B. würde die eingescannte Patienteneinwilligung den Namen des Patienten enthalten. Oder die in einem Ultraschallbild enthaltene Gerätekennung identifiziert den Arzt.)

OrgDAT sollen, wie andere Daten auch, nur so lange gespeichert werden, wie sie für die definierten Zwecke benötigt werden. Temporäre OrgDAT wie Zugriffstickets werden direkt nach Benutzung ohne Spuren gelöscht; in den zur Zugriffsüberprüfung mitgeführten Protokollen werden sie nicht benötigt. „Permanente“ OrgDAT sind solche, die zumindest eine Zeitlang benötigt werden; hier ist besonders auf mögliche Reidentifikationsrisiken zu achten. Das bedeutet insbesondere, dass die einzelnen Bestandteile der OrgDAT jeweils nur in einer einzigen Datenbank des Forschungsverbunds gehalten werden sollten.

6.5.2.5 Zusammenwirken der Module

Die Daten im Maximalmodell setzen sich zusammen aus den Daten der einzelnen Module. Auch die Datenflüsse wurden bereits weitgehend beschrieben: Das Zusammenspiel von Klinischem Modul und Studienmodul wurde in Kapitel 6.4 beschrieben, das Zusammenspiel von Studienmodul und Forschungsmodul in Kapitel 6.3. Weitgehend ähnlich dazu ist das Zusammenspiel von Klinischem Modul und Forschungsmodul, wobei die unterschiedliche Handhabung von PID_K und PID_S (bzw. SIC) zu beachten ist.

Das Zusammenspiel von Biobankenmodul und anderen Modulen wurde bereits im TMF-Datenschutzkonzept für Biomaterialbanken beschrieben und in Kapitel 5.4 zusammengefasst.

Der Gebrauch von Pseudonymen in den verschiedenen Modulen wurde zum großen Teil in Kapitel 6.1, insbesondere Unterkapitel 6.1.1 beschrieben.

6.5.3 Nutzer, Rollen und Rechte

Nutzer, Rollen und Rechte sind auch im Maximalmodell in der Regel einem einzelnen Modul zugewiesen. Übergreifende Rollen sind im IT-Bereich nicht vorgesehen und auch nicht nötig. Im organisatorischen Bereich ist vor allem die übergreifende Verantwortung für die verbundweit gültigen Richtlinien (Policies) und – soweit modulübergreifend sinnvoll – Verfahrensanweisungen

(SOPs) zu nennen; diese Rollen werden aber in der Regel nicht in der IT-Struktur direkt abgebildet.

Auch das Datenmanagement ist für die einzelnen Module, ja sogar Datenbanken, personell getrennt. Hat der Forschungsverbund zusätzlich einen zentral verantwortlichen Datenmanager oder CIO, ist darauf zu achten, dass dieser nicht Daten zur Kenntnis erhält, die ihn zur Umgehung der Pseudonymtrennung oder gar zu einer Reidentifizierung befähigen.

6.5.4 Verantwortlichkeiten

Modulübergreifende Verantwortlichkeiten betreffen

- die Definition zentraler Policies sowie
- die Genehmigung von Datenweitergaben an Forschungsprojekte.

Diese werden vom Ausschuss Datenschutz des Forschungsverbunds wahrgenommen. Ansonsten ist die Verantwortung für die einzelnen Module organisatorisch getrennt.

6.5.5 Aspekte der Realisierung

Die Anforderungen eines Forschungsverbunds im Maximalmodell an die IT-Infrastruktur sind so vielfältig, dass sie mit einem einzelnen zentral ausgerichteten EDC-System nicht zu realisieren sind. Die einzelnen Module sind in der Regel unabhängig voneinander mit geeigneten Softwaresystemen auszustatten, die aber die benötigten Kommunikationsbeziehungen und zentralen Dienste unterstützen müssen. Ein Beispiel ist das in den Kapiteln 6.5.2 und 6.1.2 b, c) beschriebene Zusammenwirken zwischen KDB, SDB und FDB.

Auch die Gewinnung, Aufbereitung, Verwaltung und Bereitstellung von Bildern erfordert eigene Software-Systeme. Enthalten die generierten Datensätze dabei im Bildmaterial selbst Daten, welche Patienten, Institutionen und Geräte identifizieren und die für die Aufnahme in die Forschungsdatenbank geschwärzt werden müssten, so muss mit den Herstellern dafür eine Änderung ihrer Software ausgehandelt werden. Für die Betrachtung und Nutzung der Bilder sollten geeignete Viewer in die Software der jeweiligen Datenbank integriert sein.

6.6 Organisatorische Regelungen

Ein Datenschutzkonzept muss immer technische und organisatorische Regelungen umfassen. Der Grundsatz „Verhindern ist besser als Verbieten“ spricht dafür, möglichst weitgehende technische Vorkehrungen zur Unterstützung des Datenschutzes zu implementieren. Aber technische Maßnahmen können

nur in einem definierten organisatorischen Rahmen ihre Wirksamkeit entfalten, der z.B. die Verantwortlichkeit klar regelt. Außerdem können technische Maßnahmen nicht alle Datenschutzanforderungen umsetzen, sondern werden immer viele Lücken lassen; hier müssen organisatorische Absicherungen, z.B. Verbote, ergänzend eingreifen.

Viele dieser organisatorischen Aspekte wurden in den bisherigen Kapiteln bereits beschrieben. In diesem Kapitel werden die nötigen Rahmenbedingungen und Regelungen eines Forschungsverbundes zusammengefasst und systematisch dargestellt.

6.6.1 Rechtsform – Forschungsverbund als juristische Person

Für eine rechtssichere Umsetzung der Regeln zu Datenschutz und Datensicherheit ist es unerlässlich, dass sich der Forschungsverbund den Status einer juristischen Person gibt, siehe auch Kapitel 4.2.3. In dieser Eigenschaft kann er für zentrale Dienste Aufträge vergeben und mit Nutzungsordnungen verbinden, welche die organisatorisch und datenschutzrechtlich relevanten Regelwerke darstellen. Die möglichen verschiedenen Rechtsformen wurden in dem Rechtsgutachten ausführlich analysiert, das die TMF im Rahmen des Biomaterialbanken-Projektes hat anfertigen lassen und das den Kern der zugehörigen Publikation [23] bildet; eine zusammengefasste Darstellung ist in [2] enthalten. Diese ist zu großen Teilen auch für medizinische Forschungsverbünde im Allgemeinen gültig und wird in entsprechend angepasster Umformulierung im Folgenden wiedergegeben.

Im akademischen Umfeld entstehen Forschungsprojekte üblicherweise durch die persönliche Initiative eines oder mehrerer Wissenschaftler. Die Trägerschaft ist dann aber in der Regel nicht an diese Person gebunden, sondern an die entsprechenden Universitäten und Kliniken. Diese beschäftigen das Personal für den Forschungsverbund und stellen Räumlichkeiten und Infrastruktur zur Verfügung. Die in diesen Einrichtungen vorhandene Infrastruktur ist einerseits ein Garant für die fachgerechte Durchführung eines Projekts, insbesondere die qualifizierte Betreuung von Daten- und Probensammlungen, andererseits besteht unter dem steigenden Kostendruck der Universitäten und Kliniken aber auch die Gefahr, dass das Forschungsvorhaben nicht weiter unterstützt wird, wenn die Leitung der Universität bzw. Klinik andere fachliche Schwerpunkte setzt oder der Initiator die Einrichtung wechselt. Auf Dauerhaftigkeit ausgerichtete Forschungsverbünde sind daher im Regelfall in einen privatrechtlichen Rahmen zu überführen und dort mittels einer geeigneten Rechtsträgerschaft zu verstetigen.

Grundsätzlich kommt jede denkbare Rechtsform für den Träger eines Forschungsverbundes in Frage. Typischerweise eignen sich in der Wissenschaft die Rechtsformen eingetragener Verein, GmbH und privatrechtliche Stiftung besonders gut für einen Forschungsverbund. Die TMF bietet mit ihrer Arbeits-

gruppe Netzwerkkoordination ein Austauschforum an, in dem dieses und weitere verwandte Themen diskutiert und Erfahrungen dazu weitergegeben werden können.

6.6.2 Allgemeine Regelungen

Satzung bzw. Gesellschaftervertrag legen die Grundlagen für die Organisation des Forschungsverbundes fest. Zu diesen Grundlagen gehören die Verantwortlichkeiten und die Ermächtigungsgrundlagen für Geschäftsordnungen. Innerhalb der Satzung oder des Gesellschaftervertrages sind die grundsätzlichen Zuständigkeiten festzulegen. Die detaillierte Ausgestaltung kann im Rahmen zusätzlicher Geschäftsordnungen erfolgen. Dabei sollte eine Unterscheidung zwischen allgemeiner Geschäftsführung und Geschäftsführung für spezielle Aufgabenfelder bezüglich Datenschutz und Forschung vorgenommen werden. Derartige Statuten zur Festlegung von Zuständigkeiten innerhalb des Forschungsverbundes sind in jedem Fall erforderlich, auch wenn er sich in öffentlich-rechtlicher Trägerschaft befindet. Ferner schließt der Träger des Forschungsverbundes Verträge bzw. Vereinbarungen mit Datenzulieferern, externen Teilnehmern und Forschungsinstitutionen sowie allen Dienstleistern, die für den Forschungsverbund tätig werden.

Wie der Verbleib des Vermögens eines Vereins muss auch der Verbleib der Daten des Forschungsverbunds in der Satzung oder im Gesellschaftervertrag geregelt sein. Für den in öffentlich-rechtlicher Hand befindlichen Forschungsverbund sollten schon zu Beginn Überlegungen angestellt werden, ob eine Übertragung der Daten an andere Institutionen oder eine Überführung in eine privatrechtliche Organisation für einen späteren Zeitpunkt vorgesehen werden soll, und entsprechende Regelungen in den Statuten getroffen werden. Hierfür können z.B. je nach Anwendungsfall Fachgesellschaften oder auch Patientenverbände in Frage kommen. Jeder Forschungsverbund sollte in seinem Regelwerk Bedingungen für seine Auflösung festlegen. Für den Fall einer Übertragung ist die Zustimmungspflicht durch die Ethikkommission, möglicherweise auch eine zuständige Fachgesellschaft zu regeln. Werden andere Regelungen gewählt, müssen diese entsprechend begründet sein.

6.6.3 Der Ausschuss Datenschutz

Die Satzung des Forschungsverbundes sieht als wichtiges Gremium neben dem Vorstand den Ausschuss Datenschutz vor, der die Regelung aller mit dem Datenaustausch und dem Datenzugang zusammenhängenden Fragen verantwortet. Die Satzung muss eine Besetzung dieses Gremiums vorsehen, die Interessenkonflikten entgegenwirkt. Sollte der Forschungsverbund als juristische Person auch über einen Datenschutzbeauftragten verfügen, sollte dieser möglichst auch Mitglied sein. Gleiches kann für Datenschutzbeauftragte der

im Forschungsverbund beteiligten Institutionen gelten. Der Ausschuss Datenschutz wird durch den Vorstand des Forschungsnetzes mit folgenden Aufgaben berufen:

- Er entscheidet mit Hilfe eines formalisierten Antragsprozesses über Art und Inhalt der Weitergabe medizinischer Daten oder wissenschaftlicher Proben an die Antrag stellenden Wissenschaftler. Mit der Bewilligung ist zu definieren
  - der auf die Forschungsaufgabe zugeschnittene Datensatz,
  - die anzuwendenden Selektionsfilter sowie
  - der Zugang zu pseudonymisierten oder anonymisierten Daten.
- Er entscheidet, ob die Benachrichtigung eines Patienten über die gewonnenen Erkenntnisse durch den zuletzt behandelnden Arzt zulässig ist. Bei besonders schwierigen Fragen kann der Ausschuss Datenschutz eine Ethikkommission zur Beratung hinzuziehen.
- Er verabschiedet die Regelwerke (Policies), die für jeden für Datenschutz und Datensicherheit relevanten Prozess zu formulieren sind, und ist verpflichtet, ihre Einhaltung im Forschungsnetz zu überprüfen und sie bei Bedarf fortzuschreiben.

Im Einzelnen sind Aufgaben des Ausschusses Datenschutz in den Kapiteln

- 4.2.3 (Verantwortlichkeiten),
- 5.2.4 (Studienmodul – Nutzer, Rollen und Rechte),
- 5.2.5 (Studienmodul – Verantwortlichkeiten),
- 5.3.2.10 (Forschungsmodul – Ergebnisse mitteilen),
- 5.3.5 (Forschungsmodul – Verantwortlichkeiten),
- 6.1.5 (ID-Management – Verantwortlichkeiten),
- 6.1.5.2 (ID-Management – Mehrere Patientenlisten an einem Standort?),
- 6.2.4 (Rechtemanagement – Verantwortlichkeiten),
- 6.3.2.9 (Kombinierter Einsatz von Studienmodul und Klinischem Modul – Machbarkeit einer Studie prüfen und Rekrutierung unterstützen),
- 6.3.4 (Kombinierter Einsatz von Studienmodul und Klinischem Modul – Verantwortlichkeiten),
- 6.4.2.8 (Kombinierter Einsatz von Studienmodul und Klinischem Modul – Rekrutierung unterstützen),
- 6.4.3 (Kombinierter Einsatz von Studien- und Forschungsmodul – Nutzer, Rollen und Rechte),
- 6.4.4 (Kombinierter Einsatz von Studien- und Forschungsmodul – Verantwortlichkeiten),
- 6.6.5.2 (Organisatorische Regelungen – Regeln für die Datenverwendung) sowie
- 6.7.4.2 (Kriterien der Verhältnismäßigkeit – Rechtemanagement)

beschrieben. Die Entscheidungen des Gremiums sollten nach dokumentierten Kriterien oder eine entsprechenden Leitlinie getroffen werden.

6.6.4 Informationelle Gewaltenteilung

Informationelle Gewaltenteilung bedeutet, dass Daten so auf verschiedene Datenspeicher mit wechselseitig nicht weisungsbefugter Administration aufgeteilt werden, dass die einzelnen Teile nicht zu einer unbefugten Reidentifikation von betroffenen Personen führen können. Beispiele hierfür sind das Identitätsmanagement, das unabhängig von den im Forschungsverbund vorhandenen Modulen betrieben wird, oder auch die Aufteilung eines Forschungsverbunds in unabhängige Module.

Erleichternd sei bemerkt, dass verschiedene Einrichtungen einer Universitätsklinik wechselseitig nicht weisungsbefugt sind, so dass etwa eine Ansiedlung zweier Datenbanken und Dienste am Klinikrechenzentrum und einem Medizininformatischen Institut in der Regel die Anforderungen an die informationelle Gewaltenteilung erfüllt. Je nach Beurteilung der Gefährdungslage eines Forschungsverbundes, siehe Kapitel 6.7 (Kriterien der Verhältnismäßigkeit), kann aber auch die Einschaltung eines externen Datentreuhänders als wirksamerer und deutlicherer Ansatz zur informationellen Gewaltenteilung angesehen werden; hierzu siehe auch Kapitel 4.2.5 (Elektronische Datentreuhänderschaft).

Einzelne Aspekte der informationellen Gewaltenteilung werden beschrieben in den Kapiteln

- 4.2.5 (Elektronische Datentreuhänderschaft),
- 4.6 (Grundprinzipien datenschutzgerechter Lösungen),
- 5.3.5 (Forschungsmodul – Verantwortlichkeiten),
- 5.4.3 (Biobankenmodul – Daten und Datenflüsse),
- 6.1.5 (ID-Management – Verantwortlichkeiten),
- 6.2 (Rechtemanagement – Einleitung),
- 6.2.4 (Rechtemanagement – Verantwortlichkeiten),
- 6.2.5 (Rechtemanagement – Aspekte der Realisierung),
- 6.4.4 (Kombinierter Einsatz von Studien- und Forschungsmodul – Verantwortlichkeiten),
- 6.7.3 (Kriterien der Verhältnismäßigkeit – Modellvarianten) sowie
- 6.7.4 (Kriterien der Verhältnismäßigkeit – Beispiele).

6.6.5 Regelwerke

Zur Konkretisierung der datenschutzrechtlichen Vorschriften, des Strafgesetzbuches, der Berufsordnung und der sonstigen berufsethischen Normen sind Regelwerke zu schaffen, auf die alle Beteiligten vertrauen können und an die das medizinisch behandelnde und forschende Personal in der Nutzung der Systeme rechtsverbindlich gebunden wird:

1. Für einen Patienten geschieht dies im Rahmen des Behandlungsvertrags mit den Ärzten oder der Klinik sowie durch die Aufklärung und eine informierte Einwilligung, Daten für den Forschungsverbund zur Verfü-

gung zu stellen. Gesunde Probanden sind analog aufzuklären und um eine Einwilligung zu bitten.
2. Für behandelnde Ärzte und klinisches Personal gelten in erster Linie die Regeln, die von den jeweiligen Kliniken unter der Verantwortung des leitenden Arztes vorgegeben sind.
3. Auch das forschende medizinische und nicht-medizinische Personal kann an die Regeln der jeweils verantwortlichen Klinik gebunden werden. Manche der Tätigkeiten, wie die Erhebung und Weiterleitung von Forschungsdaten, überschreiten die Grenzen der Klinik und müssen an Regelwerke gebunden sein, die für den gesamten Forschungsverbund verbindlich sind. Für die rechtliche Verbindlichkeit ist die Regelung der Verantwortlichkeiten durch eine geeignete Rechtsform, siehe Kapitel 6.6.1 oben, wesentliche Voraussetzung.
4. Für die zentralen Dienste – z.B. Führung der Datenbanken, Patientenliste, Qualitätssicherung und Pseudonymisierungsdienst – sind geeignete Nutzungsordnungen und SOPs mit den datenschutzrechtlich relevanten Regelwerken aufzustellen und Verträge zu schließen, welche alle Beteiligten rechtsverbindlich an die Regelwerke binden.

Insgesamt müssen die Regelwerke so gestaltet sein, dass sich aus ihnen die nötigen Rechtedefinitionen für ein wirksames Rechtemanagement (Kap. 6.2) ableiten lassen.

6.6.5.1 Verträge

Der Forschungsverbund als juristische Person schließt Verträge, um die Beteiligten an die Regelwerke zu binden:

1. mit den dokumentierenden Ärzten und ihren Mitarbeitern zur Festlegung der Anforderung an die Forschungsdaten und ihre Überlassung an den Forschungsverbund;
2. mit den Wissenschaftlern zu den Verfahren, die ihnen Zugang zu den Forschungsdaten verschaffen und sie an die regelgerechte Verwendung von Daten und biologischen Proben binden;
3. mit den zentralen Diensten und beteiligten Rechenzentren zur Regelung der Aufgaben und Pflichten, die mit dem Auftrag zur Datenverarbeitung verbunden sind. In den Verträgen soll auch die Unabhängigkeit von Datenbank-Administratoren vom forschenden Personal sichergestellt werden. Ebenso muss die wechselseitige Unabhängigkeit der verschiedenen Datenbank-Administratoren voneinander gewährleistet sein.

6.6.5.2 Regeln für die Datenverwendung

Der Wissenschaftler darf die zur Verfügung gestellten Daten ausschließlich im Rahmen der Zielsetzung seiner Arbeit und der durch das Forschungsnetz ausgesprochenen Genehmigung verwenden. Die Weitergabe der exportierten

Daten an Dritte ist generell untersagt. Für die wissenschaftliche Zusammenarbeit über die Grenzen des Forschungsnetzes hinaus sind getrennte und spezifische Regelungen mit dem Ausschuss Datenschutz des Forschungsnetzes herbeizuführen.

6.6.5.3 Sicherheitspolicy – Nutzungsordnungen

Als Regelwerke für die zentralen Dienste stellt der Forschungsverbund Nutzungsordnungen bereit, die das Sicherheitspotenzial der beschriebenen technischen Instrumente im organisatorischen Bereich verankern. Die Betreiber und die Nutzer werden über die notwendigen Maßnahmen und Abläufe informiert und zu einem planmäßigen, regelgerechten Handeln verpflichtet.

6.6.5.4 Zusammenstellung von Musterdokumenten

Ein Forschungsverbund benötigt insgesamt eine nicht unbeträchtliche Zahl von datenschutzrechtlich relevanten Regel- und Vertragswerken. Dazu gehören u.a. Policies, Verpflichtungserklärungen, SOPs und Service Level Agreements (SLA). Ein Überblick über die bei der TMF vorhandene Sammlung von einschlägigen Musterdokumenten ist im Anhang zu finden.[36]

6.6.6 Einwilligungsmanagement

Der sachgerechte Umgang mit den Patienteneinwilligungen erfordert dann einige technische Überlegungen, wenn die dort getroffenen Regelungen sich bei verschiedenen Patienten oder Probanden unterscheiden können (s. Kap. 4.2.2 „Datenschutzrechtliche Grundlagen" – „Grenzen von Einwilligungsszenarien"). Die Festlegungen, die mit der Einwilligung getroffen werden, müssen bei der jeweiligen Verwendung der Daten auf möglichst unkomplizierte Weise zur Verfügung stehen.

Zunächst wird die Einwilligung in Papierform vom aufnehmenden Arzt eingeholt und sollte in dieser Form dort auch aufbewahrt werden; bei großen und langzeitigen Forschungsverbünden kommt auch die Hinterlegung bei einem Datentreuhänder in Betracht. Falls es keine Variationsmöglichkeiten bei der Einwilligung gibt, wie es bei klinischen Studien oft der Fall ist, ist darüber hinaus kein Einwilligungsmanagement erforderlich.

Anders sieht es aber aus, wenn patientenindividuelle Festlegungen zu berücksichtigen sind. Bei jeder beabsichtigten Datenverwendung muss in jedem Einzelfall feststehen, was erlaubt ist. Daher muss ein Feld der OrgDAT dafür vorgesehen werden, detaillierte Informationen zur Einwilligung abzubilden, den Wunsch nach Wissen oder Nichtwissen und bei einer abgestuften Ein-

36 Anhang siehe unter http://www.tmf-ev.de/datenschutz-leitfaden

willigungsmöglichkeit etwa die gewählte Stufe (s. Kap. 4.4.2). Auch Ausschlüsse müssen dort festgehalten werden, was in den meisten Fällen ein Freitextfeld erforderlich macht. Diese Erweiterung der OrgDAT ist im Klinischen, Studien-, Forschungs- und Biobankenmodul relevant.

Zu beachten ist, dass das Mitführen dieser Daten in Einzelfällen ein erhöhtes Reidentifizierungsrisiko bedeuten kann; z.B. könnte, wenn in einer Forschungsdatenbank und in einer Probenbank eine einzigartige identische Einwilligungsregelung festgehalten wird, die Trennung der Pseudonyme unwirksam werden. Für eine solche Situation ist die Einrichtung eines zentralen Einwilligungsmanagements, etwa kombiniert mit dem Identitätsmanagement, zu empfehlen.

Hinweise zum Einwilligungsmanagement sind in den vorangegangenen Kapiteln

- 5.1.2.1 (Klinisches Modul – Patienten in das Klinische Modul aufnehmen),
- 5.1.2.10 (Klinisches Modul – Rekrutierung unterstützen),
- 5.2.2.1 (Studienmodul – Patienten aufklären und Einwilligung einholen),
- 5.3.2.4 (Forschungsmodul – Machbarkeit einer Studie prüfen),
- 6.3.2.2 (Kombinierter Einsatz von Studien- und Klinischem Modul – Patienten in Klinisches Modul oder Studienmodul aufnehmen),
- 6.4.2.1 (Kombinierter Einsatz von Studien- und Forschungsmodul – Patienten in das Studienmodul aufnehmen),
- 6.4.2.3 (Kombinierter Einsatz von Studien- und Forschungsmodul – Datenqualität im Studienmodul sichern),
- 6.4.2.7 (Kombinierter Einsatz von Studien- und Forschungsmodul – Machbarkeit einer Studie prüfen),
- 6.4.2.8 (Kombinierter Einsatz von Studien- und Forschungsmodul – Rekrutierung unterstützen),
- 6.5.2.1 (Maximalmodell – Patienten aufnehmen) sowie
- 6.5.2.4 (Maximalmodell – Organisatorische Daten – Dokumentation des Patientenwillens)

zu finden. Unproblematisch in technischer Hinsicht ist die Rücknahme einer Einwilligung. Wird eine Einwilligung aber nachträglich abgeändert, müssen die entsprechenden Änderungen natürlich an allen einschlägigen Stellen der OrgDAT nachgetragen werden.

6.6.7 Besonderheiten bei der Umsetzung

Für den Aufbau der organisatorischen Strukturen sind nach den Grundsätzen der Verhältnismäßigkeit verschiedene Varianten möglich; siehe hierzu die detaillierten Kriterien in Kapitel 6.7. Als Beispiel sei ein Vorschlag für den Ausschuss Datenschutz, insbesondere bei seltenen Erkrankungen, erwähnt: Dieser muss in kleineren Verbünden nicht ein gesondertes Gremium sein, sondern könnte vom Vorstand bzw. Leitungsgremium unter Einbeziehung des

Datenschutzbeauftragten verkörpert werden. Dies ist insbesondere dann angemessen, wenn im Verbund, z.B. in einem Register, nur vorher festgelegte Auswertungen vorgesehen sind.

Die von der TMF als Muster angebotenen Vorlagen für Verträge usw. sind im Anhang zusammengestellt und werden online angeboten[37].

Für das Kontaktmanagement könnte der Einsatz kommerzieller CRM-Software von Interesse sein; Erfahrungen hiermit liegen im TMF-Umfeld aber noch nicht vor.

6.7 Kriterien der Verhältnismäßigkeit

6.7.1 Redundanz und Aufwand

Datenschutzmaßnahmen sind unter der Maßgabe der Verhältnismäßigkeit zu sehen. Auf technischer Ebene können Sicherheitsmaßnahmen sehr aufwändig, damit aber auch sehr teuer gestaltet werden. Unbeliebter Aufwand entsteht insbesondere durch die Schaffung von Redundanzen. Redundanz ist aber ein wichtiger Aspekt in Sicherheitskonzepten, wenn es um hochsensible Daten geht: Wenn eine Sicherheitsmaßnahme unwirksam wird, soll eine „sichere Rückfallposition" erreicht werden. Unwirksam kann eine Sicherheitsmaßnahme aus verschiedenen Gründen werden, beispielsweise:

- nicht regelkonformes Verhalten einzelner Beteiligter,
- unbefugte Kooperation verschiedener Beteiligter oder eines Beteiligten mit einem Externen,
- Ausfall einer technischen Komponente oder
- Kompromittierung einer technischen Komponente.

Beispiele für Redundanzen von Bedeutung für dieses Datenschutzkonzept sind:

- Kombination eines Verbots (z.B. in einer vertraglichen Regelung) mit einer technischen Barriere (z.B. durch Zugriffskontrolle) oder Überprüfung (z.B. durch Protokollierung von Handlungen),
- mehrfache unabhängige Pseudonymisierung,
- Zugriffsschranken für Ärzte trotz der dreifachen Absicherung der ärztlichen Schweigepflicht durch die Androhung strafrechtlicher, zivilrechtlicher und standesrechtlicher Folgen oder
- trotz Pseudonymisierung verschlüsselte Übermittlung von Daten über das Internet.

Verhältnismäßigkeit bedeutet in der Regel nicht, dass ein kontinuierlicher Sicherheitsparameter mehr oder weniger hoch angesetzt wird, sondern dass Redundanzen vermehrt oder abgebaut werden.

37 http://www.tmf-ev.de/datenschutz-leitfaden

Unter den für medizinische Forschungsverbünde vorgesehenen Maßnahmen führt eine sehr feingliedrige Trennung der Verantwortung für einzelne Funktionen der Daten-, Proben- und Rechteverwaltung zu solchen erwünschten Redundanzen. Sie stößt aber dort auf Grenzen der Angemessenheit oder sogar der Durchführbarkeit, wo Forschungsprojekte von relativ kleinen Organisationseinheiten durchgeführt werden. Ein „kleines" Forschungsnetz kann mit wenig Redundanz in technischen und organisatorischen Datenschutzmaßnahmen betrieben werden, wenn es als Angriffsziel weniger attraktiv ist, weniger Angriffspunkte bietet, weniger „Geheimnisträger" hat, organisatorisch übersichtlich ist und mit nur wenigen Komponenten auskommt, in deren Zusammenspiel sich Sicherheitslücken verbergen könnten.

Grundsätzlich sind bei allem Aufwand immer Fälle einer unberechtigten Reidentifizierung konstruierbar. Es muss hier der mögliche Schaden mit dem Aufwand ins Verhältnis gesetzt werden. Daher sind Abwägungen zu treffen zwischen dem Umfang der gespeicherten Daten, dem Risiko einer Reidentifizierung, der Komplexität der Organisation und dem möglicherweise bestehenden Interesse für einen Übergriff. Für alle Forschungsverbünde gilt aber, dass mangelnde Ressourcen kein Argument für mangelhafte Datenschutzmaßnahmen sein können. Insbesondere müssen sich die Zuordnungen von Pseudonymen zu Personen (Identitätsmanagement) und die Forschungsdaten mit ganz wenigen Ausnahmefällen in getrennter Verantwortung befinden.

6.7.2 Parameter für die Risikoabschätzung

Die für die Risikoabschätzung relevanten Aspekte eines medizinischen Forschungsverbundes werden hier in vier Dimensionen gegliedert, die nicht notwendig unabhängig voneinander sind. Es kann keine einfache Formel geben, die aus konkreten Werten für die Parameter die Höhe des Risikos berechnet. Manche Parameter können sich sogar gegenläufig auswirken, indem sie an einer Stelle das Risiko erhöhen, es aber an anderer Stelle senken. Sinn dieser Parameterliste ist vielmehr, für einen konkreten Forschungsverbund potenzielle Schwachstellen aufzudecken. Eine Auswirkung der Risikoabschätzung könnte z.B. sein, dass für den einen Forschungsverbund redundante Sicherheitsmaßnahmen als notwendig angesehen werden, für einen anderen dagegen die Redundanz verringert werden kann; oder dass eine Abschwächung an einer Stelle durch zusätzliche Maßnahmen an anderer Stelle kompensiert wird.

6.7.2.1 Risikodimension „Größe des Forschungsverbundes"

Diese wird durch folgende vier Parameter ausgedrückt:

1. **Fallzahl**: Es ist wohl schwierig, hier explizite allgemein gültige Grenzen zu ziehen. Ein Register oder eine Forschungsdatenbank mit wenigen 100 Patienten ist sicher als klein, eines mit über 10.000 Patienten sicher

als groß einzustufen. Es gibt auch gegenläufige Effekte: Mit der Fallzahl steigt die Attraktivität für einen unbefugten Zugriff auf den Datenbestand des Forschungsverbunds; andererseits sinkt das individuelle Reidentifizierungsrisiko aus MDAT und AnaDAT, da es weniger einzigartige Merkmalskombinationen gibt.

2. **Einzugsbereich und Anzahl der Daten- oder Probenquellen**: Ein Forschungsverbund, der deutschlandweit von Hunderten von Arztpraxen Daten sammelt, ist sicher anders zu bewerten als eine Probensammlung in einem Kliniklabor, die nur Blutproben von Patienten einer bestimmten Fachabteilung enthält. Eine einfachere Logistik bietet weniger Angriffspunkte; bei weniger Datenquellen bestehen bessere Möglichkeiten zur dezentralen Organisation, z.B. der Patientenliste, was je nach Umständen auch ein Sicherheitsgewinn sein kann.
3. **Finanzielle Ausstattung und Zahl der Beschäftigten**: Ein sparsam gefördertes öffentliches Forschungsprojekt ohne kommerzielle Ambitionen oder Aussichten hat sicher wenig Möglichkeiten, komplizierte Schutzmaßnahmen umzusetzen; dadurch steigt die Wahrscheinlichkeit von Sicherheitslücken. Hier ist eine besonders sorgfältige Prüfung unter dem Gesichtspunkt der Verhältnismäßigkeit nötig; mangelnde finanzielle Ausstattung darf kein Argument zur Absenkung des Datenschutzstandards sein.
4. **Komplexität**: Mit steigender Komplexität wächst die Wahrscheinlichkeit für unbeabsichtigte Wechselwirkungen, Sicherheitslücken und Datenlecks.

6.7.2.2 Risikodimension „Brisanz des Forschungsverbunds"

Diese Risikodimension ist hoch mit der potenziellen Attraktivität für einen Angreifer korreliert und kann durch folgende sechs Parameter beschrieben werden:

1. **Art der Erkrankung**: In unserer Gesellschaft werden z.B. psychiatrische Erkrankungen und HIV als stigmatisierend angesehen. Hier spielt auch die öffentliche Beachtung des Forschungsprojekts eine Rolle, da sie sich unmittelbar auf das Vertrauen der Patienten auswirkt. Krankheiten mit hoher Morbidität könnten z.B. für Krankenversicherer interessant sein.
2. **Vollständigkeit der Erfassung**: Je vollständiger die Erfassung, desto größer die Wahrscheinlichkeit, dass eine bestimmte Person erfasst ist, desto geringer aber auch die Wahrscheinlichkeit für einzigartige Merkmalskombinationen. Beispielhafte Fragen: Wird nur eine (zufällig ausgewählte) Kohorte erfasst oder handelt es sich um ein Register mit dem Anspruch auf Vollzähligkeit? Werden alle Probanden mit einer seltenen Erkrankung erfasst? Werden alle Probanden aus einer bestimmten Region erfasst, vielleicht alle Patienten einer Klinik?

3. **Umfang der Datenerhebung**: Je umfangreicher die gespeicherten Datensätze sind, desto mehr unterscheiden sich die Einzelfälle, desto höher ist also das Reidentifizierungsrisiko. Beispielhafte Fragen: Werden nur wenige medizinische Daten erfasst? Werden nur wenige Analysedaten erzeugt, z.B. keine genetischen Daten? Welche soziodemografischen Daten werden erfasst? Werden Angaben erfasst, die Angehörige betreffen?
4. **Forschungsziele**: Diese bestimmen die Brisanz eines Forschungsvorhabens wesentlich mit. Beispielhafte Fragen: Sind genetische Analysen vorgesehen, die ja auch Angehörige der Probanden oder ganze ethnische Gruppen betreffen? Dadurch steigt sowohl die Attraktivität für einen unbefugten Zugriff samt der Zahl der dadurch Betroffenen als auch das Reidentifizierungsrisiko. Sollen Forschungsergebnisse in wichtigen Fällen an die Patienten oder Probanden rückgemeldet werden? Sind Langzeitbeobachtungen der Patienten geplant? In diesen beiden letzteren Fällen muss der „Rückweg“ zum Patienten durch geeignete Pseudonymisierung offen gehalten werden, was u.U. zusätzliche Angriffspunkte schafft und das Reidentifizierungsrisiko erhöht.
5. **Art der gespeicherten Daten oder des gelagerten Materials**: Wie einfach ist damit eine Reidentifizierung möglich? Zu berücksichtigen sind z.B. soziodemographische Daten, feingranulare Anamnesedaten, charakteristische Bilddaten von offensichtlichen Missbildungen, Proben oder extrahierte DNA.
6. **Einzigartigkeit von Daten oder Proben**, z.B. durch eine Monopolstellung des Forschungsverbunds in einem bestimmten Bereich.

6.7.2.3 Risikodimension „Organisation des Forschungsverbunds“

Die hier beschriebenen neun Parameter wirken sich ganz wesentlich auf die Beurteilung der Verhältnismäßigkeit aus und sind z.T. relativ leicht zu beeinflussen, wenn das Vorhaben sorgfältig geplant wird.

1. **Beschlagnahmesicherheit**: Man muss nach Dierks [20] davon ausgehen, dass eine rechtlich beschlagnahmefeste Aufbewahrung zentral gespeicherter Daten bei verteilter Datenerhebung nur in wenigen Ausnahmefällen möglich sein wird. Andererseits bedingt das Schutzprinzip der informationellen Gewaltenteilung (vgl. Kap. 4.6), dass entweder medizinische oder identifizierende Daten außerhalb der behandelnden Einrichtung aufbewahrt werden müssen und so der Beschlagnahme unterliegen können.
2. **Präzision der Aufklärung und Einwilligung**: Je weniger bestimmt die Forschungsziele benannt werden können, desto mehr ist durch Verstärkung der Sicherheitsmaßnahmen oder weitergehende Informationstrennung zu kompensieren.
3. **Verteiltheit der Zulieferung** (vgl. auch Kap. 6.7.2.1 Nr. 2): Hier gibt es gegenläufige Effekte: mit der Verteiltheit steigt einerseits die Informationstrennung, andererseits auch die Zahl der Angriffspunkte.

4. **Verteiltheit der Datenspeicherung und Probenlagerung**. Auch hier gilt: Mit der Verteiltheit erhöht sich die Informationstrennung und steigt gleichzeitig die Zahl der Angriffspunkte.
5. **Dauer der Datenspeicherung und Probenlagerung**: Das Risiko von Angriffen ist direkt proportional zu dieser Dauer.
6. **Umfang geplanter Nacherhebungen**. Ist eine erneute oder gar häufig wiederholte Kontaktierung der Patienten oder Probanden vorgesehen? Das erfordert eine komplexere Logistik und erhöht die Zahl der Angriffspunkte sowie die Gefahr von Datenlecks und unbefugter oder sogar unbeabsichtigter Reidentifizierung.
7. **Qualität der Policies und SOPs sowie der vertraglichen Regelungen mit Externen**: Hier sind Abwägungen zwischen technischen und organisatorischen Maßnahmen zu treffen und mögliche oder nötige Redundanzen zu diskutieren.
8. **Vertrauenswürdigkeit einer datenspeichernden oder -verarbeitenden Stelle**: Z.B. ist eine Bundesbehörde, deren Mitarbeiter strengen und öffentlich kontrollierbaren Regeln unterliegen, u.U. vertrauenswürdiger im Sinne eines Datenschutzkonzepts als ein privatwirtschaftlich organisierter Betrieb, dessen Regeln sich bei einer Geschäftsübernahme kurzfristig ändern können oder dessen Datenbestand im Konkursfall auf nicht vorhersagbare Weise weitergegeben wird.
9. **Vorgesehene Monitoring- oder anderweitige Kontrollverfahren**: Eine institutionalisierte und genau festgelegte Nachprüfung aller Verfahrensschritte (z.B. ein Monitoring-Verfahren) kann mit anderen Datenschutzmaßnahmen redundant sein und diese eventuell ersetzen.

6.7.2.4 Risikodimension „Verbindung mit externen Daten“

Hierfür sind zwei Parameter relevant, die kaum beeinflusst, nicht einmal vollständig kontrolliert werden können:

1. **Abgleichmöglichkeit oder -pläne mit anderen Datenquellen oder Registern**: Hier ist einem eventuell erhöhten Reidentifizierungsrisiko durch technische oder organisatorische Maßnahmen zu begegnen.
2. **Vorhandensein von Referenzdateien**: Solche Dateien, z.B. mit genetischen Fingerabdrücken oder soziodemographischen Daten, können zu einer unmittelbaren Reidentifizierung von Daten des Forschungsverbundes führen, so dass die Zusammenführung mit technischen oder organisatorischen Maßnahmen verhindert werden muss; beim Datenexport sind entsprechende Fragen zu stellen und Regelungen zu treffen.

Die Möglichkeiten zum externen Datenabgleich können niemals vollständig und für alle Zukunft beurteilt werden; sie betreffen aber genau das Hauptanliegen eines Datenschutzkonzepts, das Reidentifizierungsrisiko zu vermeiden. Daher ist bei diesen Parametern eine besonders vorsichtige Einschätzung notwendig. Nicht erreichbar ist in der Regel *k*-Anonymität [34]. Abzuwägen sind die Möglichkeiten zur vollständigen, faktischen oder nur formalen Anonymi-

sierung – für die Abgrenzung und Problematik der Verwendung dieser Begriffe sei auf das Glossar in diesem Werk verwiesen – und ihre Konsequenzen bzw. kompensatorische Maßnahmen.

6.7.3 Modellvarianten

Bei der Beschreibung der Module und ihrer Komponenten wurden an verschiedenen Stellen bereits Modellvarianten und abweichende Organisationsformen, sogar Zusammenlegungen von im Standard-Konzept getrennten Funktionen oder Datenspeichern als Möglichkeiten aufgeführt. Bei Abweichungen vom Standardkonzept und insbesondere Vereinfachungen der technischen und organisatorischen Maßnahmen ist immer eine Einzelfallprüfung unter Anwendung der Kriterien erforderlich.

Erleichternd für die Zulässigkeit von Abweichungen ist die Etablierung eines Monitoring- oder Audit-Verfahrens. Solche Verfahren gelten ohnehin als die beste Methode, Regelverstöße von Insidern aufzudecken [38].

Stufen für die Datentrennung sind:

1. getrennte Datenbank-Tabellen,
2. getrennte Datenbanken,
3. getrennte Datenhoheit sowie
4. externer Datentreuhänder.

Stufe 1 ist nur bei monozentrischen klinischen Studien oder im Behandlungszusammenhang angemessen und in dieser Form heute oft in Krankenhausinformationssystemen vorzufinden; sie schützt im wesentlichen davor, dass ein Systemverwalter Identitätsdaten und medizinische Daten zusammen sieht, ohne es zu wollen. Außerdem lässt sich für alle anderen Datenbanknutzer auf dieser Basis leicht eine differenzierte Zugriffsregelung aufbauen.

Als Beispiel für Stufe 2 ist bei institutionsinterner Langzeitforschung (Beispiel: Datawarehouse im Krankenhaus) der Aufbau einer getrennten Datenbank mit einfacher Pseudonymisierung ausreichend, obwohl es sich vom Charakter der Datensammlung her um eine Forschungsdatenbank handelt. Ebenso kann Stufe 2 für eine kleine institutionsinterne Biomaterialbank angemessen sein [2]. Diese Stufe der Datentrennung schützt zusätzlich vor einem Angreifer, der Zugang zu einer der Datenbanken hat, z.B. auf einem unzulänglich gelöschten ausrangierten Datenträger.

Stufe 3 ist der empfohlene Normalfall für die meisten medizinischen Forschungsverbünde und führt bei geeigneter organisatorischer Regelung zu einer angemessenen informationellen Gewaltenteilung.

Stufe 4 kann bei besonders sensiblen Erkrankungen verhältnismäßig sein, etwa um dem Misstrauen von Patienten oder Patientenverbänden gegen die medizinische Forschung entgegenzuwirken.

Das Maximalmodell ist angemessen, wenn in einem großen Forschungsverbund vielfältige Projekte aller Art mit komplexer Datenlogistik durchgeführt werden sollen. Hierfür relevante Kriterien sind:

- Notwendigkeit der langfristigen (Pseudonymisierung) Aufbewahrung von Daten oder Proben (über Behandlungs- oder Studienkontext hinaus), langfristige Forschungsvorhaben wie Spätfolge- oder Lebensqualitätsstudien, Kohortenstudien und
- größere Patienten- oder Probandenzahlen (z.B. keine seltene Erkrankung).

In der Mehrheit der Fälle ist allerdings eine „kleinere“ Lösung angemessen. Viele Forschungsverbünde, z.B. Netzwerke für seltene Erkrankungen, benötigen nur eine Klinische Datenbank, eventuell in Kombination mit einer Biomaterialbank. Verbünde, bei denen im Wesentlichen epidemiologische Fragen verfolgt werden, können mit einer Forschungsdatenbank auskommen. Hier sind jeweils die bei der Beschreibung der Einzelmodule vorgeschlagenen Lösungen mit eventuell nötigen, sachgerecht begründbaren Modifikationen angemessen. Bei der Wahl des passenden Modells spielen – auch im Sinne des Datenschutzes – Überlegungen zur Praktikabilität eine wichtige Rolle.

6.7.4 Beispiele

Um die in den vorigen Kapiteln auf einer eher abstrakten Ebene angestellten Überlegungen für die praktische Anwendung nutzbar zu machen, werden hier zahlreiche konkrete Anwendungsbeispiele vorgestellt. Entscheidend ist bei allen Varianten, dass das Reidentifizierungsrisiko nicht erhöht wird.

6.7.4.1 Identitätsmanagement

Ist die Aufteilung des ID-Managements in Patientenliste und Pseudonymisierungsdienst nötig? Wird für die Patientenliste ein externer Treuhänder eingesetzt, kann dieser den Pseudonymisierungsdienst auch zusätzlich übernehmen, wenn dieser auf einem eigenen Rechner mit räumlicher und personeller Trennung von der Patientenliste organisiert wird. Bei PID-Vergabe an der Datenquelle – bei kleineren Projekten sinnvoll – kann der PID als Pseudonym dienen. Ein zusätzlicher Pseudonymisierungsdienst ist dann verzichtbar.

Darf ein PID an der Datenquelle bekannt sein? Ja, wenn er dort erzeugt wird. Bei klinischen Studien ist das so vorgesehen (SIC oder evtl. PID_S). Auch wenn der Forschungsverbund kein Klinisches Modul betreibt, sondern seine Daten direkt im Forschungsmodul speichert, ist die Kenntnis des PID an der Quelle unschädlich, wie auch im „alten“ Modell B vorgeschlagen [1].

Weitere Hinweise zu einzelnen Punkten finden sich wie folgt:

- Soll die Patientenliste zentral oder dezentral geführt werden? Siehe Kapitel 6.1.5.1.
- Wo soll die Patientenliste angesiedelt sein? Siehe Kapitel 6.1.5.2.

- Wo soll der Pseudonymisierungsdienst angesiedelt sein? Siehe Kapitel 6.1.5.4.
- Soll ein SIC zentral oder dezentral erzeugt werden? Siehe Kapitel 6.1.1.1.

6.7.4.2 Rechtemanagement

Die folgenden Fragestellungen zum Rechtemanagement sind zu berücksichtigen:

- Sollen Arzt-Identitäten (ADAT) pseudonymisiert werden? Argumente hierzu stehen in einem zusätzlichen Hinweis in Kapitel 6.1.1.2.
- Können die ADAT bei den MDAT gespeichert werden? Das ist in der Regel (vgl. Kap. 6.1.5.1) nicht ratsam, da es Hinweise für eine Reidentifizierung geben kann. Eine Ausnahme wäre denkbar, wenn jeder meldende Arzt für sehr viele Patienten zuständig ist, z.B., wenn nur große Schwerpunktkliniken Daten liefern.
- Sollen Nutzdaten (MDAT) durch das Identitätsmanagement oder an ihm vorbei geleitet werden? (vgl. Kap. 6.1.2 b). Das ist vom Datenschutz aus gesehen – bei adäquater Implementierung – äquivalent und kann daher nach Praktikabilität und Performanz entschieden werden.
- Ist für das Nutzer- und Rechtemanagement ein Verzeichnisdienst notwendig? Das wurde in den Kapiteln 6.2.1.2 und 6.2.5.1 diskutiert.
- Welche Rollenkonflikte können bei Ärzten im Forschungsverbund auftreten und wie soll man mit ihnen umgehen? Hierzu macht das Kapitel 6.2.3.3 einige Aussagen.
- Wo soll das Rechtemanagement angesiedelt sein? Dazu sei auf Kapitel 6.2.4 verwiesen. Unabhängig von der technischen Implementierung unterliegt es der zentralen Verantwortung unter Kontrolle des Ausschusses Datenschutz.
- Ist die Nutzung einer PKI im medizinischen Forschungsverbund anzuraten? Dazu sei auf Kapitel 6.2.5.2 verwiesen.
- Welche Werkzeuge sollen zur Spezifikation von Richtlinien und Regeln eingesetzt werden? Dazu wurden in Kapitel 6.2.5.4 Hinweise gegeben.
- Welche Werkzeuge sollen zur Rechteverwaltung eingesetzt werden? Gesichtspunkte dazu wurden in Kapitel 6.2.5.5 erörtert.

6.7.4.3 Bilddaten

Für die Ansiedlung von Bilddaten gibt es verschiedene Varianten:

- zum Klinischen Modul, wenn eine Referenzbefundung mit möglicher Rückwirkung auf den Patienten vorgesehen ist;
- zum Studienmodul, wenn Bilder direkt in einer klinischen Studie benötigt werden, insbesondere zur Referenzbefundung (Befundung von Bildern durch Referenzradiologen);

- zum Forschungsmodul, wenn die Bilder nur zu Vergleichszwecken bei der Befundung oder als Referenzmaterial für Forschung und Lehre dienen sollen – nur bei *qualitätsgesicherten* Bildern (oder Daten);
- in einem Extra-Modul, wenn übergreifende Zwecke verfolgt werden und die Ansiedlung in einem der anderen Module ein zu hohes Reidentifizierungsrisiko bedeutet.

Hauptkriterium für eine eigenständige im Gegensatz zu einer integrierten Bilddatenbank ist die Erkennbarkeit einer Person im Bildmaterial, wenn dieses außerhalb des Behandlungszusammenhangs gespeichert wird; hierzu sei auch auf die Diskussion von Bilddaten in den Kapiteln 6.5.1 und 6.5.2.3 hingewiesen.

Eine weitere Abwägung der Verhältnismäßigkeit ist erforderlich, wenn Bilddaten für die weitere Nutzung zugänglich gemacht werden sollen (Referenzmaterial, wissenschaftliche Auswertung). Für die Frage allerdings, ob der Export von Bildern einem direkten Zugriffsrecht vorzuziehen ist, sind neben dem Datenschutz auch technische Argumente zu berücksichtigen (Dateigröße); oft, insbesondere zu Referenzzwecken, ist schon wegen der Dateigröße oder der Performanz ein Export nicht sinnvoll. Es soll aber auch verhindert werden, dass mit exportierten Daten eine externe Datenbank aufgebaut wird. Daher ist es meistens besser, einen Online-Zugriff für „Forschungsprojekte" einzurichten, der über passende Zugriffsregelungen gestaltet wird.

6.7.4.4 Biomaterialbanken

Beispiele zu Abwägungen der Verhältnismäßigkeit im Zusammenhang mit Biomaterialbanken im Forschungsverbund sind im generischen Datenschutzkonzept für Biomaterialbanken beschrieben [2].

6.7.4.5 Sonstiges

Für den Zugriff auf Forschungsdaten durch externe Wissenschaftler bis hin zu einem Public-Use-File ist die Hierarchie von Möglichkeiten – in Anlehnung an die Regelungen des statistischen Bundesamtes – zu berücksichtigen, die in Kapitel 5.3 vorgestellt wurde. In der Regel werden für Public-Use-Files nur sehr stark vergröberte Daten bereitgestellt werden können, mit denen man Fragen beantworten kann, die für den Forschungsverbund selbst keine Relevanz mehr besitzen, die aber im öffentlichen Interesse sein könnten.

Sollen Daten beim Versand über das Internet zusätzlich verschlüsselt werden, auch wenn sie pseudonymisiert sind? Ja, denn einerseits kann das Reidentifizierungsrisiko pseudonymisierter Daten bei unbekannten Angreifern nicht eingeschätzt werden. Andererseits wird durch die verschlüsselte Übermittlung die Pseudonymisierung keinesfalls überflüssig, da sie ja den Personenbezug vor dem Empfänger schützen soll. Außerdem würde die Pseudonymisierung

die Daten auch noch schützen, wenn das Verschlüsselungsverfahren, das für die Kommunikation verwendet wird, kompromittiert wird; selbst wenn ein Angreifer die Daten in verschlüsselter Form gespeichert hätte, wären sie dann immer noch vor ihm geschützt.

Beim Studienmodul lassen sich die Varianten „zentrales Datenmanagement" auf der einen, „separate Studiendatenbank für jede Studie" auf der anderen Seite und entsprechend die Verwendung von PID_S bzw. nur SICs vom Datenschutzgesichtspunkt aus beide zufrieden stellend umsetzen, siehe die Diskussion in Kapitel 5.2. Die Entscheidung für eine der Varianten kann also unter Praktikabilitätsgesichtspunkten getroffen werden.

Wann die Einrichtung einer temporären Datenbank zur Qualitätssicherung angemessen ist und was dabei zu beachten ist, wird in Kapitel 6.8 beschrieben. Entscheidend ist hier, dass es sich um ein etabliertes Verfahren handelt, das innerhalb des Forschungsverbundes reguliert ist, und dass keine längerfristige Datenspeicherung vorgesehen ist; d.h., die temporäre Zusammenführung von sonst getrennten Daten wird durch Regelungen kompensiert.

6.7.5 Seltene Erkrankungen

Da Netzwerke für seltene Erkrankungen ein wichtiger Schwerpunkt der Forschungsförderung sind, diese aber einerseits durch geringe Ressourcen, andererseits durch extrem kleine Fallzahlen und vielfältige Fragestellungen gekennzeichnet sind, werden Empfehlungen für solche Forschungsverbünde hier explizit zusammengefasst.

In Europa bezeichnet man eine Krankheit als selten, wenn sie weniger als einen unter 2000 Menschen im Laufe seines Lebens trifft [39]. Das bedeutet, dass in Deutschland auch über längere Zeiträume hinweg oft nur wenige hundert Fälle einer bestimmten Krankheit auftreten. Von den ungefähr 30.000 bekannten Krankheiten werden 5.000 bis 7.000 zu den seltenen Erkrankungen gerechnet. Zählt man diese zusammen, sind sie allerdings kein seltenes Phänomen; in Deutschland leiden rund 4 Millionen Menschen an einer seltenen Erkrankung. Häufig handelt es sich um schwere Krankheiten, die eine aufwändige Behandlung und Betreuung erfordern, für die Betroffenen und ihre Familien mit hoher Belastung verbunden sind und oft schon im Kindes- oder Jugendalter mit dem Tod enden. Ein typisches Beispiel ist der kindliche Lebertumor, der im Zeitraum zwischen 1980 und 2004 nur bei 382 Kindern im Alter von bis zu 15 Jahren auftrat. Für die schwere aplastische Anämie waren es im gleichen Zeitraum in der gleichen Population 280 Fälle [40].

Bei vielen seltenen Erkrankungen ist die ihnen zugrunde liegende Ursache ungeklärt. Man nimmt an, dass bei etwa 80% genetische Veränderungen ursächlich sind, allerdings sind die jeweils betroffenen Gene häufig noch nicht identifiziert. Für einige Erkrankungen gibt es bisher noch nicht einmal Ansätze zur Erforschung der Krankheitsursachen [7].

Folglich ist in vielen Fällen die medizinische Versorgung der Kranken noch unbefriedigend. Um aber in der klinischen Forschung valide Ergebnisse zu erzielen, sind Patientenzahlen erforderlich, die einzelne Fachleute und Zentren kaum erreichen können. Zur Verbesserung der Versorgung der Patienten ist es daher unumgänglich, die Forschung zur Klärung der Krankheitsursachen sowie zur Entwicklung, Validierung und Etablierung von Diagnoseverfahren und Therapiekonzepten zu konzentrieren und zu intensivieren [39]. Gleiches gilt für die epidemiologische Forschung, insbesondere wenn Varianten einer Erkrankung untersucht und multifaktorielle Ursachen geklärt oder regionale Unterschiede und zeitliche Trends erkannt werden sollen. Sofern Behandlungsdokumentationen und Proben nicht systematisch und flächendeckend gesammelt werden, besteht keine Chance, eine seltene Krankheit erfolgreich zu erforschen. Daher ist die Vernetzung zwischen behandelnden und forschenden Ärzten sowie medizinischen Einrichtungen eine wesentliche Voraussetzung für den wissenschaftlichen Fortschritt.

Als Musterbeispiel können hier die großen Erfolge im Bereich der Pädiatrischen Onkologie und Hämatologie dienen [41], die durch eine solche systematische Rückkopplung der Forschung in die Versorgung erreicht wurden. Die im Netzwerk vorhandene diagnostische und therapeutische Spitzenkompetenz für die jeweilige Krankheit steht für die Behandlung aller teilnehmenden Patienten zur Verfügung, so z.B. die zentrale Referenzdiagnostik (Labor, Pathologie, Radiologie) oder Konsiliardienste durch die Studienleitung für Therapie-Entscheidungen. Andererseits profitieren diese führenden Fachleute durch die wesentlich verbesserte Datenlage und die Zuarbeit aller Behandler für die weitere Forschung.

Im vitalen Interesse der Patienten selbst liegt es auch, einen möglichst großen Kreis von Fachleuten einzubeziehen. Und für sie ist es ebenfalls wichtig, dass ihre Daten und Proben nicht in abgegrenzten Projekten „vergeudet“ werden, sondern in einem gemeinsamen Pool möglichst effizient verwertet werden.

Bei den meisten seltenen Erkrankungen (dies gilt insbesondere für sehr seltene Erkrankungen) ist die rechtlich gebotene Trennung zwischen den Daten zur Behandlung, zur klinischen Forschung und zur epidemiologischen Forschung kontraproduktiv für alle Beteiligten: Die Behandlungsdaten sind für die Forschung ebenso wichtig, wie die Forschungsdaten die Behandlung unterstützen können, und jeder Patient ist immer auch zugleich für die Forschung von Bedeutung. Auch die Patienten selbst haben oft ein großes Interesse an Forschungsprojekten, da neue Behandlungsoptionen aufgrund der notwendigen systematischen Evaluation nur im Rahmen einer Studie zur Verfügung stehen. In einer solchen Situation kann die Dokumentation im Rahmen eines Forschungsprojekts einer elektronischen Patientenakte gleichkommen, die auch für künftige Auswertungen genutzt werden kann.

Zusammengefasst sind die Versorgungs- und Forschungsziele eines Forschungsverbundes für seltene Erkrankungen:

- Koordination der Forschung zu einer Erkrankung mit Akkumulation ausreichender Patientenzahlen, um statistisch sinnvolle Auswertungen, die Untersuchung von Sonderfällen und Varianten, von regionalen Unterschieden und zeitlichen Trends sowie genetische Analysen und die Rekrutierung für künftige klinische Studien zu ermöglichen.
- Langzeitbegleitung der Patienten durch eine möglichst vollständige und standardisierte Dokumentation.
- Optimierung der Therapie und der Betreuung durch den Aufbau eines Behandlungsnetzes unter Beteiligung der führenden Fachleute (horizontale Vernetzung), Konsultationssystem, Erarbeitung von Leitlinien zur Diagnostik und Therapie, Kooperation der Fachzentren untereinander und mit niedergelassenen Ärzten, die in der Regel sehr selten oder erstmalig mit einer seltenen Erkrankung konfrontiert sind.
- Sammlung von Referenzfällen.
- Förderung der direkten Kommunikation von Experten untereinander sowie mit weniger erfahrenen Ärzten, z.B. in einem Expertenforum (s. Kap. 5.1.2.5).
- Bereitstellung von Informationen für Patienten (vertikale Vernetzung) über Ursachen, Diagnostik, Verlauf, Therapiemöglichkeiten; Einbeziehung von Selbsthilfegruppen, insbesondere auch Förderung der Patienten-Community.

Eine Vollerfassung von Patienten mit bestimmten Behinderungen oder lebensbestimmenden Erkrankungen ist aber – auch vor dem Hintergrund der geschichtlichen Erfahrungen in Deutschland – gesellschaftspolitisch heikel. Eine mögliche Stigmatisierung ist, je nach Krankheitsbild, nicht auszuschließen. Erschwerend kommt hinzu, dass viele seltene Erkrankungen mit auffälligen, nicht zu verbergenden körperlichen Erscheinungsformen einhergehen, die eine wirksame Anonymisierung oder Pseudonymisierung der Daten erschweren, z.B. körperliche Fehlbildungen.

Aus diesen Rahmenbedingungen ergeben sich folgende Überlegungen für einen auch aus Sicht des Datenschutzes adäquaten Aufbau eines Forschungsverbundes für seltene Erkrankungen:

Grundsätzlich ist ein solcher Forschungsverbund ein typischer Anwendungsfall für ein Klinisches Modul, wobei hier zweckmäßigerweise nur eine einzige zentrale Klinische Datenbank (meist als Register bezeichnet) aufgebaut werden sollte. In der Regel wird aber auch eine zugehörige Biomaterialbank benötigt. Das Zusammenspiel dieser beiden Komponenten ist im generischen Datenschutzkonzept für Biomaterialbanken [2] beschrieben. Üblich und sinnvoll ist es dabei, eine Gruppe verwandter Krankheiten in einem gemeinsamen Forschungsverbund zu untersuchen.

Wichtig und in der Regel von allen Beteiligten gewünscht ist gerade bei seltenen Erkrankungen die enge Kooperation mit Patientenorganisationen und Selbsthilfegruppen, soweit diese schon vorhanden sind; andernfalls könnte es gerade ein Ziel des Forschungsverbunds sein, solche Gruppen ins Leben zu rufen und zu unterstützen. Da oft Kinder die Betroffenen sind, ist zunächst die Einwilligung der Eltern relevant, die, sobald das Kind die nötige Einsichtsfähigkeit erlangt hat, durch dessen eigene Einwilligung zu ersetzen ist. In den (aller Erfahrung nach seltenen [7]) Fällen, wo diese verweigert bzw. zurückgezogen wird, sind geeignete Anonymisierungsmaßnahmen durchzuführen, oder gar, wenn eine wirksame Anonymisierung unmöglich ist, die entsprechenden Falldaten zu löschen.

Auf jeden Fall sollte die Patientenliste unabhängig von der Datenbank geführt werden; sie könnte auch die LabIDs verwalten, wenn diese nicht ohnehin von den Laboren vergeben werden. Hierfür bilden sich zur Zeit im Umfeld der TMF zentrale Dienstleister an Universitätskliniken heraus, die auch die Patientenlisten verschiedener Forschungsverbünde verwalten; wichtig dabei ist aber, dass es genügend viele davon gibt und somit eine angemessene Verteilung der damit verbundenen informationellen Gewalt gewährleistet ist. Die Frage, ob es sinnvoll ist, um die Zugehörigkeit einer Person zu einer bestimmten Diagnosegruppe zu verschleiern, die Patientenlisten mehrerer seltener Erkrankungen zusammenzufassen, wurde in Kapitel 6.1.5.2 diskutiert und negativ beantwortet

Die Pseudonymisierung beim Export von Daten zur statistischen Auswertung ist in diesem Modell eine Funktion der Klinischen Datenbank, ebenso wie die Funktionen zur „Rekrutierung“, d.h. der Gewinnung von Patienten für neue klinische Studien. Die Gestaltung dieser Funktion wird in den Kapiteln 5.1.2.9 und 5.1.2.10 beschrieben.

Software-Produkte „von der Stange“, die zum Betrieb einer Klinischen Datenbank oder eines Registers, insbesondere für seltene Erkrankungen, direkt geeignet sind, sind bisher nicht erhältlich. Hier besteht noch Entwicklungsbedarf, entsprechende Arbeiten und Projekte sollten von der TMF koordiniert werden. Dies kann, ebenso wie die zentrale Bereitstellung von Dienstleistungskapazität für den Betrieb von Patientenlisten, wesentlich dazu beitragen, der Ressourcenknappheit der Forschungsverbünde für seltene Erkrankungen zumindest teilweise zu begegnen.

6.8 Qualitätssicherung

Unter Qualitätssicherung wird in diesem Text die Sicherstellung der Datenqualität verstanden. Andere Aspekte des Qualitätsmanagements wie Struktur-, Prozess- und Ergebnisqualität sind zwar für medizinische Forschungsverbünde auch von Bedeutung, spielen für das Datenschutzkonzept aber kei-

ne unmittelbare Rolle. Die Datenqualitätssicherung dagegen muss notwendigerweise oft mit personenbezogenen Daten arbeiten und ist daher datenschutzrelevant.

Damit die medizinische Forschung aus den verfügbaren Daten valide Ergebnisse gewinnen kann, müssen die Daten hohe Anforderungen an Genauigkeit, Vollständigkeit und Korrektheit erfüllen. Daher ist die Datenerhebung und Datenverarbeitung in medizinischen Forschungsverbünden in der Regel mit einer oder mehreren Stufen der Qualitätssicherung verbunden; deren Umfang und Komplexität sind für das einzelne Projekt durch das Studiendesign und die Normen, denen es sich unterwirft, definiert, für den gesamten Forschungsverbund durch das Zusammenspiel der Module und Komponenten. Dabei geht es immer um die Ergänzung und Korrektur fehlerhafter, fehlender, unvollständiger und unplausibler Daten. Bei epidemiologischen Studien setzen die Forscher selbst bei der Studienplanung die Anforderungen und Verfahren fest. Bei klinischen Studien sind die Anforderungen in „Standard Operation Procedures“ (SOPs) durch generelle Richtlinien festgelegt.

Typische Datenfehler sind

- Schreibfehler, wie Zahlendreher,
- Einträge in falschen Datenfeldern,
- fehlende Einträge,
- inhaltliche Irrtümer, wie Fehldiagnosen.

Manche dieser Fehler können automatisch durch die Erfassungssoftware abgefangen werden: Ein Monat 13 existiert z.B. nicht; eine Zahl im Namensfeld muss ein Irrtum sein. Fehldosierungen von Medikamenten können zumindest einen Warnhinweis auslösen. Schreibfehler in Namen oder Fehldiagnosen sind dagegen automatisch kaum zu erkennen. Daher ist neben möglichst guten Fehlererkennungsalgorithmen der Software in der Regel auch eine Nachkontrolle durch Menschen nötig. Hierfür ist zunächst das Datenmanagement der jeweiligen Datenbank zuständig, je nach Herkunft oder geplanter Verwendung der Daten sind weitere Kontrollen mit mehr oder weniger aufwändigen Verfahren notwendig.

Die Prozesse der Qualitätssicherung sind in den allgemeinen Richtlinien des Forschungsverbundes zu beschreiben und in Form von SOPs genau festzulegen. Insbesondere ist dort anzugeben, wo personenbezogene Daten benötigt werden und wie mit diesen umgegangen wird. Hinweise dafür geben die folgenden Kapitel.

6.8.1 Klinisches Modul

Im Behandlungskontext werden Daten primär zu Abrechnungszwecken erhoben; eine darüber hinaus gehende Dokumentation ist wegen des damit ver-

bundenen Arbeitsaufwandes in der Regel nicht möglich. Das führt dazu, dass z.B. Nebendiagnosen, die für die Abrechnung keine Rolle spielen, nicht notiert werden; möglicherweise wird sogar die Hauptdiagnose im Hinblick auf den Erlös „optimiert". Solche Daten sind für die medizinische Forschung nahezu unbrauchbar; nicht einmal grobe Krankheitsstatistiken können damit zuverlässig erstellt werden. Sollen die Daten für Auswertungen irgendwelcher Art verwendet werden, ist hier bereits eine erste Stufe der Qualitätssicherung vonnöten. Daher sind direkt bei der Dateneingabe im Klinischen Modul eines Forschungsverbunds qualitätssichernde Maßnahmen einzuführen, die als Nebeneffekt auch die klinische Befundkommunikation verbessern. Solche Maßnahmen bestehen aus Algorithmen zur Überprüfung der Vollständigkeit und Plausibilität der klinischen Daten, die unmittelbar bei der Eingabe durch die Erfassungssoftware ausgeführt werden, sowie aus anschließenden im Behandlungsprozess vorhandenen qualitätssichernden Maßnahmen. Da Online-Eingabe und Abfrage ausschließlich durch den behandelnden Arzt erfolgen kann, sind asynchrone Mechanismen zur Datenüberprüfung zunächst entbehrlich, ein Rückgriff auf die Klinik (oder Rückfrage-Management) beim Export von Forschungsdaten ist oft nicht notwendig, insbesondere, wenn die Klinische Datenbank die einzige zentrale Datenbank des Forschungsverbunds ist, wie es z.B. bei chronischen oder seltenen Erkrankungen häufig zutrifft und im Modell A des alten generischen TMF-Datenschutzkonzept beschrieben wurde [1].

Das Studiendesign eines versorgungsnahen Registers oder einer Beobachtungsstudie kann aber auch ein geeignetes Monitoring-Verfahren einschließen, um verbleibende Fehler zu eliminieren. Ferner ist ein Rückmeldeverfahren notwendig, wenn die Daten für andere Module oder Projekte exportiert und dort Fehler entdeckt werden. Im Klinischen Modul kann also auch, wie in einem Studienmodul (s.u.), ein ausgefeiltes Qualitätssicherungsverfahren mit Rückfrage-Management, Monitoring und Auditing vorgesehen werden.

6.8.2 Studienmodul

In klinischen Studien, bei denen durch die Studienplanung eine bestimmte Datenqualität verbindlich vorgeschrieben ist, ist ein komplexes, zu Beginn der Studie detailliert festgelegtes Qualitätssicherungsverfahren die Regel. Dieses besteht aus konsiliarischer Beratung, Rückfrage-Management, Monitoring, Safety-Management und Audit.

Für die Nutzung in klinischen Studien nach AMG entsprechen fertig entwickelte Softwaresysteme üblicherweise hinsichtlich Funktionsumfang, Qualitätssicherung und Dokumentation den umfangreichen gesetzlichen Vorgaben bzw. den Kriterien der Good Clinical Practice (GCP). Hierzu gehört z.B. die Funktion eines umfassenden Audit-Trails, in dem alle Änderungen an Datensätzen nachvollziehbar gespeichert werden und der dem Monitor zugänglich sein muss.

6.8.2.1 Konsiliarische Beratung

Ein wichtiges Element bei klinischen Studien ist die Begleitung der Behandlung durch einen erfahrenen Studienarzt. Alle Daten des Patienten werden durch ihn bezüglich einer richtigen und adäquaten Behandlung begutachtet. Der Studienarzt kann den behandelnden Arzt gegebenenfalls konsiliarisch beraten. Wenn diese Beratung vom Studienarzt oder anderem ärztlich geführten Personal mit Patientenkontakt durchgeführt wird, geschieht dies im Regelfall in Kenntnis der Identität des betroffenen Patienten. In jedem Fall steht die konsiliarische Beratung in engem Zusammenhang mit der Behandlung des Patienten. Hierbei anfallende Datenänderungen sind in der Studiendatenbank zu dokumentieren.

6.8.2.2 Rückfrage-Management

Als zweite Stufe der Qualitätssicherung klinischer Forschungsdaten (nach der Eingabekontrolle) ist ein Rückfrage-Management vorgesehen. Dieses wird vom Datenmanagement ausgelöst und ist mit einer Kommunikation pseudonymer Daten verbunden, wobei ein Kommunikationspartner die Zuordnung des Pseudonyms (hier SIC oder PID_S) zum Patienten kennt und der andere im Regelfall nicht. So können im zentralen Datenmanagement Rückfragen zu den Daten eines Patienten formuliert werden, ohne dass die Identitätsdaten des Patienten hierfür benötigt werden. Wenn diese Rückfragen vom Studienarzt oder anderem ärztlich geführten Personal mit Patientenkontakt bearbeitet werden, geschieht dies im Regelfall in Kenntnis der Identität des betroffenen Patienten.

6.8.2.3 Monitoring

In einer dritten Stufe werden Monitore eingesetzt, die die eingegebenen Daten vor der Auswertung noch einmal auf Vollständigkeit und Plausibilität überprüfen. Dabei wird auch der Dateneingabevorgang hinterfragt und die Übereinstimmung mit den Quelldaten optisch nachvollzogen. Daher müssen Monitore sowohl Zugang zu den von ihnen zu überprüfenden zentralen Patientendaten wie auch zu den Quelldaten in den beteiligten Zentren und behandelnden Einrichtungen haben. Da dieser Nutzerkreis außerhalb des Behandlungsverhältnisses steht und gleichzeitig auch Zugriff auf personenbezogene Unterlagen mit Klartext-Identitätsdaten hat, müssen Patienten vor Aufnahme in die Studie darüber aufgeklärt werden und können nur nach einer entsprechenden Einwilligung teilnehmen.

6.8.2.4 Safety-Management

Im Rahmen der allgemeinen Qualitätssicherung in klinischen Studien werden alle unerwarteten Studienereignisse je nach ihrem Schweregrad an den Spon-

sor und an die zuständigen Behörden gemeldet. Hierbei gibt es behördliche Verpflichtungen gemäß dem AMG. In der Regel erfolgen diese Meldungen ausschließlich mit pseudonymisierten Daten. Eine Überprüfung der Quelldaten erfolgt dann im Rahmen des allgemeinen Monitoring.

6.8.2.5 Audit

Als Audit werden allgemein Untersuchungsverfahren bezeichnet, die dazu dienen, Prozessabläufe hinsichtlich der Erfüllung von Anforderungen und Richtlinien zu bewerten. Die Audits werden im Regelfall von speziell hierfür geschulten, unabhängigen und externen Fachleuten durchgeführt. Im Kontext von medizinischen Forschungsprojekten, insbesondere klinischen Studien ist ein Audit eine weitere Stufe der Qualitätssicherung. Hierbei werden sämtliche Prozesse auf Übereinstimmung mit Studienplan, Richtlinien, SOPs und anderen verbindlichen Festlegungen – auch hinsichtlich Datenschutzmaßnahmen – geprüft. Ein Zugriff auf konkrete Daten ist, im Gegensatz zum Monitoring, allenfalls stichprobenartig nötig; ein Personenbezug muss dabei nicht offenbart werden.

6.8.3 Forschungsmodul

Wird eine Forschungsdatenbank aus einer ausreichend qualitätsgesicherten Klinischen Datenbank oder einer Studiendatenbank gespeist, kann man in der Regel eine genügende Datenqualität annehmen. Kommen Daten auf anderem Wege in die Forschungsdatenbank, ist vor der Übernahme der Informationen ein vorgeschaltetes Qualitätssicherungssystem erforderlich, welches im Feedback zur Klinik oder Datenquelle Mängel in der Plausibilität und Vollständigkeit der Daten minimiert. Dieses muss besondere Datenschutzanforderungen erfüllen, da viele qualitätssichernde Prozesse nach einer Pseudonymisierung der Daten nicht mehr sinnvoll durchgeführt werden können und daher nur mit einem Personenbezug möglich sind (s.u.). Kompliziert wird das Verfahren durch die Möglichkeit, dass spätere Daten zum gleichen Fall in der Regel einen neuen Qualitätssicherungsprozess für den Gesamtdatensatz auslösen.

Zusätzlich zu diesen Routine-Verfahren ist auch ein Korrektur-Prozess vorzusehen, der später nachgereichte Korrekturen übernimmt, die von der Datenquelle, aus einem anderen Modul des Forschungsverbunds oder von Betroffenen selbst in Wahrung seines datenschutzgesetzlichen Berichtigungsrechts angestoßen werden.

6.8.3.1 Allgemeine Anforderungen an das Verfahren (bei Daten aus dem Behandlungszusammenhang)

Die Qualitätssicherung erfordert einen unbehinderten Austausch von Informationen zwischen dem dokumentierenden Arzt, der die Daten beim Patien-

ten und aus seiner Kranken- und Behandlungsgeschichte erhebt, und der prüfenden Stelle. Die prüfende Stelle kann die Stelle sein, welche die Daten sammelt und speichert, oder eine dazwischen geschaltete Stelle, die das Monitoring übernimmt; es kann aber auch eine eigene, unabhängige Stelle dafür eingerichtet werden. Sie wird im Folgenden als QS-Service bezeichnet.

Liegt die Datenquelle im Behandlungszusammenhang, so gibt der dokumentierende Arzt bzw. die erhebende Klinik die Daten mit einem Patientenidentifikator (PID) weiter, der auch vom QS-Service gespeichert und benutzt wird, um den entsprechenden Datensatz in der Kommunikation mit der Klinik zu identifizieren. Die datenschutzrechtliche Zulässigkeit beruht darauf, dass dem QS-Service ein Zugriff auf die entsprechenden IDAT, die in der Klinik liegen, verwehrt wird. Sie entspricht damit einem bei der Speicherung von Forschungsdaten in Studienzentren oder übergeordneten Forschungsdatenbanken weithin genutzten Standard.

6.8.3.2 Workflow für die Qualitätssicherung von der Behandlung in die Forschungsdatenbank

Zusammengefasst läuft folgender Prozess ab, in dem die verschiedenen Zustände der Daten begrifflich unterschieden werden (s. Abb. 22):

- Der QS-Service erhält von der Klinik die mit dem PID verknüpften „Erhebungsdaten".
- Er benötigt auch den Vergleich mit früher erhobenen Daten, die bereits in der Forschungsdatenbank gespeichert sind; diese werden als „Kontextdaten" temporär zur Verfügung gestellt. Dazu übergibt er eine Liste der aktuellen PIDs an den Pseudonymisierungsdienst, der diese in eine entsprechende PSN-Liste umwandelt.

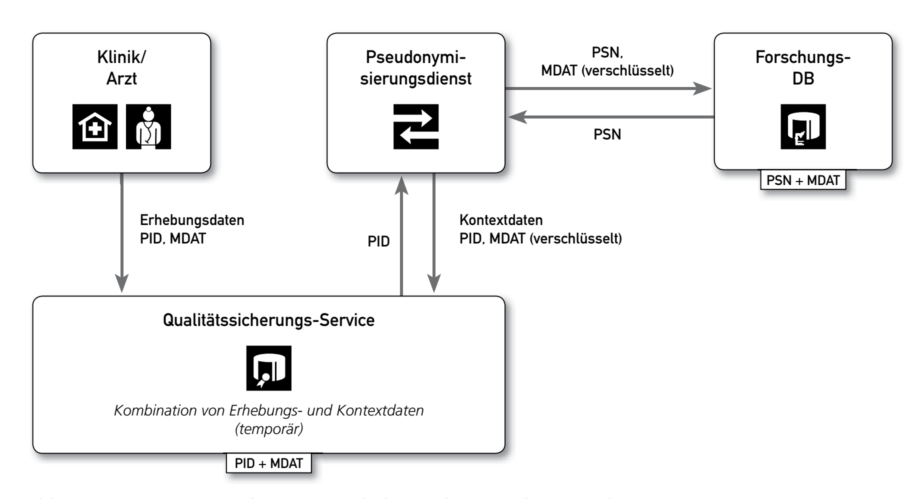


Abb. 22 Der QS-Service übernimmt Erhebungsdaten und Kontextdaten.

- Der Pseudonymisierungsdienst sendet die PSN-Liste an die Forschungsdatenbank.
- Die Forschungsdatenbank sendet die zugehörigen Kontextdaten (mit dem öffentlichen Schlüssel des QS-Service verschlüsselt) an den Pseudonymisierungsdienst.
- Der Pseudonymisierungsdienst ersetzt die PSN wieder durch die entsprechenden PIDs und sendet diese, zusammen mit den immer noch verschlüsselten Kontextdaten an den QS-Service zurück.
- Der QS-Service führt in Kommunikation mit der Klinik die Qualitätssicherung für die mit PID gekennzeichneten Daten durch. Die Behandlungseinrichtung kann dabei auf die Patientenakte und die Original-Dokumentation zugreifen.
- Der QS-Service übergibt die korrekten oder korrigierten Erhebungsdaten über den Pseudonymisierungsdienst der Forschungsdatenbank, wo sie als Forschungsdaten dauerhaft gespeichert werden.
- Danach wird der temporäre Bestand an Erhebungsdaten und Kontextdaten gelöscht.

Der QS-Service führt für seine Aufgaben eine temporäre Datenbank, die in sequentiellen Verfahren mit neuen Erhebungsdaten gefüllt wird, die im Rahmen der Qualitätssicherung laufend abgearbeitet werden. Plausible oder durch Korrektur plausibel gemachte Datensätze werden nach Abschluss der Teilprozesse in Forschungsdaten transformiert und aus der temporären Datenbank gelöscht.

6.8.3.3 Daten aus externen Quellen

Im Forschungsmodul sind, insbesondere bei epidemiologischen Fragestellungen, oft auch Datenabgleiche mit externen Datenquellen bis hin zu Meldeämtern, Gesundheitsämtern und Standesämtern vorgesehen. Diese sind im Rahmen des Qualitätssicherungsprozesses zu definieren und müssen natürlich die rechtlichen Rahmenbedingungen (s. Kap. 4.3.4) einhalten. Im Gegensatz zu dem in Kapitel 6.8.3.2 beschriebenen Verfahren muss hierbei auf Identitätsdaten zurückgegriffen werden. Um die für den QS-Service definierten Regeln nicht aufzuweichen, ist zu empfehlen, dass die externe Kommunikation über die Patientenliste oder eine weitere, eigens für diesen Zweck beauftragte Datentreuhänderstelle abgewickelt wird.

Enthält der Forschungsverbund auch ein Klinisches Modul oder ein Studienmodul, so können die Ergebnisse eines solchen externen Datenabgleichs auch wieder Rückmeldungen oder Rückfragen in dieses auslösen.

6.8.3.4 Einrichtung eines QS-Service

Der QS-Service als besonderer Dienst muss nur in Forschungsverbünden extra aufgesetzt werden, die Daten direkt in eine Forschungsdatenbank aufnehmen,

ohne dass diese zuvor die Qualitätssicherungsprozesse eines Klinischen oder Studienmoduls durchlaufen haben. Er benötigt eine eigene Datenbank, in der Daten während des laufenden Prozesses mit einem PID gekennzeichnet gehalten und nach Beendigung dieses Prozesses (Übergabe qualitätsgesicherter Daten an die Forschungsdatenbank) gelöscht werden. Der Datenbestand ändert sich also laufend, wobei die einzelnen Datensätze nur temporär vorgehalten werden.

Der temporäre Bestand wird auf diese Weise ständig nach der Zahl der Datensätze und in den Inhalten modifiziert; da er niemals einen Zustand erreicht, der nach anderen Regeln als denen der Qualitätssicherung als konsolidiert gelten könnte, ist es nicht möglich, die Daten in anderer als der vorgesehenen Art und Weise zu nutzen. Es besteht kein Anreiz, den Bestand regelwidrig z.B. für irgendwelche Forschungsfragen zu gebrauchen.

Es ist ein Regelwerk festzulegen, nach dem der zulässige Gebrauch des temporären Datenbestands beschrieben und die Einhaltung der Regeln von Dritten (z.B. von Seiten des betrieblichen Datenschutzes) geprüft und bestätigt werden kann.

6.8.4 Patientenliste

Auch die Führung einer Patientenliste im Forschungsverbund kann als Teil der Qualitätssicherungsbemühungen angesehen werden (s. Kap. 6.1.2. a). Hier ist die eindeutige Identifikation des Patienten durch einen fehlertoleranten Record-Linkage-Algorithmus gemeint. Da dieser nicht perfekt arbeiten kann, ist die regelmäßige (z.B. einmal jährlich, je nach Zeithorizont des Forschungsverbunds oder einzelner Projekte) Überprüfung der Patientenliste auf Synonyme (clerical review) vorzusehen; entsprechende Korrekturen sind an die einzelnen Module weiterzugeben.

6.8.5 Rückmeldungen von Datenfehlern

Eine Datenkorrektur in einem Modul des Forschungsverbundes oder in der Patientenliste zieht unter Umständen die Notwendigkeit von Korrekturen in anderen Modulen nach sich. Gleiches gilt, wenn ein Betroffener sein Berichtigungsrecht wahrnimmt. Für diese Korrekturen sind geeignete Rückmeldungsprozesse zu definieren.

6.8.5.1 Nutzung der Daten einer Forschungsdatenbank zum Zwecke der Qualitätssicherung

Wird das Forschungsmodul mit anderen Modulen (z.B. dem Studienmodul oder Klinischen Modul) gekoppelt, so können schon vorhandene Daten eines Patienten aus dem Forschungsmodul zum Zwecke der Qualitätssicherung ge-

nutzt werden. Eine genaue Beschreibung befindet sich im Kapitel 6.4 zum kombinierten Einsatz von Studien- und Forschungsmodul.

6.8.5.2 Kombination von Studienmodul und Klinischem Modul

Die entsprechenden Rückmeldungsprozesse zur Korrektur von Datenfehlern wurden in Kapitel 6.3 ausführlich beschrieben.

6.8.5.3 Kombination von Klinischem Modul und Forschungsmodul

Hier lassen sich die nötigen Prozesse analog zur Kombination von Studien- und Forschungsmodul beschreiben.

7 Zusammenfassung und Ausblick[38]

Das Ziel eines Datenschutzkonzepts ist immer das Austarieren unterschiedlichster und scheinbar gegensätzlicher Anforderungen: Es gilt, eine Balance zwischen der Umsetzung eines angemessenen und realisierbaren Schutzniveaus, welches Forschung ermöglicht und nicht behindert, auf der einen Seite und der Verhinderung von Datenmissbrauch auf der anderen Seite zu finden. Um Forscher in die Lage zu versetzen, diesen Ansprüchen und Anforderungen zu genügen, hat die TMF erstmals 2003 mit den Arbeitskreisen „Wissenschaft“ und „Gesundheit und Soziales“ der Datenschutzbeauftragten des Bundes und der Länder abgestimmte generische Datenschutzkonzepte für die medizinische Verbundforschung vorgelegt [1]. Dies hat, zusammen mit dem 2006 zusätzlich veröffentlichten generischen Datenschutzkonzept für Biomaterialbanken [2] und unterstützt durch das Beratungsangebot der Arbeitsgruppe Datenschutz der TMF, zu einer deutlichen Vereinfachung der Erarbeitung, Abstimmung und Umsetzung von Datenschutzkonzepten in der Verbundforschung geführt.

38 Dieses Kapitel entstand erst nach der Abstimmung des Leitfadens mit den Datenschützern der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und ist somit von dem Empfehlungsbeschluss der 87. Konferenz in Hamburg am 27. und 28. März 2014 nicht mit umfasst (s. http://www.datenschutz.hessen.de/dg011.htm#entry4196).

Nicht zuletzt die umfangreich in der TMF zusammengetragene Erfahrung aus der Anwendung der bisherigen Konzepte hatte jedoch auch einen deutlichen Überarbeitungsbedarf aufgezeigt. Der vorliegende Leitfaden baut auf diesen Erfahrungen auf und hat dabei bewährte technische und organisatorische Schutzprinzipien der bisherigen Konzepte beibehalten. Gleichzeitig trägt er aber mit der neuen und weitreichenden Modularisierung dem Bedarf nach einer breiteren Unterstützung verschiedener Anwendungsfälle Rechnung. Die modulare Konstruktion erlaubt die Konzeption und Umsetzung von Maßnahmen, die an den jeweiligen Zweck angepasst sind und die auch alle damit verbundenen technischen, organisatorischen und rechtlichen Rahmenbedingungen reflektieren. Unter der Berücksichtigung detailliert aufgeschlüsselter Kriterien der Verhältnismäßigkeit kann eine Feinjustierung des Datenschutzkonzepts und der damit verbundenen Aufwände erfolgen.

Eine wichtige rechtliche Trennlinie verläuft zwischen der Datenverwendung zu Zwecken der Patientenversorgung und dem Nutzungskontext der Forschung. Diese rechtliche Trennlinie korrekt abzubilden ist besonders dann schwierig, wenn der Forschungsprozess eng verzahnt mit der Versorgung der betroffenen Patienten abläuft. Solche Anwendungsfälle lassen sich mit dem Klinischen Modul abbilden, welches sowohl einen namensbezogenen Zugriff auf die Patientendaten im Rahmen der Behandlung ermöglicht, als auch den Aufbau einer pseudonymen Datensammlung für spätere Forschungszwecke unterstützt. Die Trennlinie zwischen Versorgung und Forschung wird somit innerhalb dieses Moduls abgebildet. Das Klinische Modul entspricht damit weitgehend der im bisherigen Konzept [1] als „Modell A“ bezeichneten Lösung für versorgungsnahe Forschung.

Eine weitere und häufig weniger bekannte Trennlinie ist zu beachten, wenn die Daten primär für Forschungszwecke erhoben werden. Diese verläuft zwischen Forschungsprojekten mit konkreter und schon bei der Planung bekannter Zielsetzung und festlegbarer Laufzeit und solchen Daten- und Probensammlungen, die später auch für heute noch nicht absehbare Forschungsfragestellungen zur Verfügung stehen sollen. Letztere haben häufig keine konkret begrenzte Laufzeit. Ein gutes Beispiel für Forschungsprojekte mit begrenzter Laufzeit und konkreter Zweckbindung sind klinische Arzneimittelstudien, in denen auch der Auswertungsplan schon vor dem Einschluss des ersten Patienten festgelegt ist. Im vorliegenden Leitfaden wurden alle notwendigen Informationen für ein angepasstes Datenschutzkonzept für solche Forschungsvorhaben im Studienmodul zusammengefasst.

Wenn Daten weniger eng zweckbezogen gesammelt und aufbewahrt werden, wie etwa in epidemiologischen Registern, so sind die mit der dann notwendigerweise langfristigen Speicherung verbundenen erhöhten Risiken in Bezug auf die informationelle Selbstbestimmung durch zusätzliche technische und organisatorische Maßnahmen auszubalancieren. Wie dies erreicht werden kann, beschreibt das Forschungsmodul, welches damit die in dem bisherigen

generischen Konzept [1] in „Modell B“ dargestellte versorgungsferne Forschung eher „wissenschaftszentrierter Forschungsnetze“ abbildet und auch dort erstmals entwickelte Schutzmaßnahmen übernimmt.

Ebenfalls folgenschwer ist die Entscheidung, ob in einem Forschungsprojekt auch oder primär Proben gesammelt, gelagert und ausgewertet werden sollen. Der Aufbau einer Biobank erfordert die Umsetzung besonderer technischer und organisatorischer Schutzmaßnahmen, u.a. auch aufgrund des hohen Reidentifizierungspotenzials von Proben, die im Regelfall das gesamte Genom des betroffenen Probanden enthalten. Hierfür wurde von der TMF das generische Datenschutzkonzept für Biomaterialbanken entwickelt [2]. Im vorliegenden Leitfaden wird in dem Biobankmodul auf dieses Konzept verwiesen, so dass über diese Integration auch eine Verzahnung von Biobanken mit anderen Forschungsprojekten und deren Datensammlungen möglich wird.

Der Leitfaden beschreibt aber nicht nur die Anwendungsfälle und Umsetzungsmöglichkeiten innerhalb der einzelnen Module, sondern gibt darüber hinaus auch einen Einblick in übergreifende Szenarien mit der Interaktion mehrerer Module, bis hin zu einem Maximalmodell mit allen Formen von Daten- und Probensammlungen innerhalb eines Forschungsverbunds. Damit steht nun eine umfangreiche Handreichung für alle Forscher, Koordinatoren, IT-Experten, Geschäftsführer, Juristen und andere an heutigen biomedizinischen Forschungsprojekten Beteiligte zur Verfügung, die die Konzeption und Umsetzung einer datenschutzgerechten Lösung deutlich vereinfachen und beschleunigen kann.

Bei der ganz konkreten Erstellung eines Datenschutzkonzepts samt Einwilligungserklärung und zugehöriger Policies hilft ein elektronischer Anhang, in dem sowohl bestehende Unterstützungsangebote der TMF als auch mit diesem Leitfaden neu erstellte Dokumente unter einer Online-Adresse zusammengestellt und verlinkt wurden. Dieses zusätzliche Angebot kann zudem künftig noch weiter wachsen, wenn weitere beispielhafte Datenschutzkonzepte oder andere hilfreiche Unterlagen zur Verfügung gestellt werden.

Die biomedizinische Forschung entwickelt sich jedoch in rasantem Tempo weiter. Heute ist kaum abzusehen, welche Möglichkeiten sich der Forschung in zehn Jahren eröffnen und welche methodischen Ansätze dann die Forschungslandschaft prägen. Neben den technischen und methodischen Entwicklungen ist aber auch mit gesetzlichen Veränderungen zu rechnen, wie sie z.B. mit dem Entwurf einer einheitlichen europäischen Datenschutzgrundverordnung bereits am Horizont aufscheinen. Entsprechend ist auch ein solcher Leitfaden mit seinen Empfehlungen und Handlungsanweisungen kontinuierlich weiterzuentwickeln und immer wieder an neue Gegebenheiten anzupassen.

Die Arbeit an diesem Leitfaden hat deutlich gezeigt, dass sich die Heterogenität der Forschungslandschaft und der relevanten Anwendungsfälle sowie die

Besonderheiten der technischen, organisatorischen und rechtlichen Rahmenbedingungen biomedizinischer Forschung nicht ohne eine Austauschplattform, wie sie die TMF darstellt, erfassen, bearbeiten und abbilden lassen. Kein Expertenteam kann heute diese Bandbreite an Themen aus eigener Anschauung überblicken. Hierfür wird auch in Zukunft immer eine ständige Rückkopplung mit Forschern und Experten aus unterschiedlichsten Forschungsprojekten notwendig sein.

Immer wieder neue medizinische Forschungsprojekte finden sich in der TMF zusammen und nutzen sie als Austauschplattform, in die sie ihre spezifischen und womöglich neuen Anforderungen einbringen können. Dabei zu Tage tretende Schwierigkeiten mit der Umsetzung des Datenschutzleitfadens können bei der kontinuierlichen Weiterentwicklung des generischen Datenschutzkonzepts und seiner Module berücksichtigt werden. Neue oder modifizierte Lösungsvorschläge werden dann unter dem Dach der TMF und in Abstimmung mit Medizinrechtlern und Datenschutzbeauftragten entwickelt und publiziert, zum Nutzen wiederum nachfolgender Forschungsprojekte.

Verzeichnisse

Glossar

Die nachfolgenden Begriffserläuterungen aus dem Bereich der medizinischen Forschungsverbünde orientieren sich an folgender Grundstruktur:

- Definition
- Erläuterung (z.T. mit Beispielen)
- Verweise (Nachweise, Hinweise, weiterführende Angaben)

Im Einzelfall können Glossar-Einträge jedoch von diesem Grundmuster abweichen. Formulierungen zu klinischen Studien wurden zum Teil von R. Meinert und I. Stamm (KKS Mainz, heute IZKS Mainz[39]) übernommen. Für einige Einträge wurde auf Inhalte oder auch Formulierungen aus der Wikipedia zurückgegriffen. An den entsprechenden Stellen ist dies mit Hilfe von Fußnoten gekennzeichnet. Das Glossar ist alphabetisch geordnet.

ADAT

Definition: Daten, die einen teilnehmenden Arzt des → Forschungsverbunds beschreiben, insbesondere Name und Kontaktdaten.

---

39 www.izks-mainz.de

Erläuterung: ADAT werden meist als Teil der →OrgDAT behandelt.

AE

siehe →unerwünschtes Ereignis.

AMG

siehe →Arzneimittelgesetz.

AMG-Studie

Definition: Eine →Studie, die dem →Arzneimittelgesetz (AMG) unterliegt. Dort definiert als „jede am Menschen durchgeführte Untersuchung, die dazu bestimmt ist, klinische oder pharmakologische Wirkungen von Arzneimitteln zu erforschen oder nachzuweisen oder Nebenwirkungen festzustellen oder die Resorption, die Verteilung, den Stoffwechsel oder die Ausscheidung zu untersuchen, mit dem Ziel, sich von der Unbedenklichkeit oder Wirksamkeit der Arzneimittel zu überzeugen."

Erläuterung: Eine solche Studie ist eine der Voraussetzungen dafür, dass ein Arzneimittel zugelassen wird. →Nichtinterventionelle Prüfungen werden hiervon nicht erfasst. Die Anwendung von GCP (→Good Clinical Practice) ist vorgeschrieben.

Anonymisierung

Definition: Anonymisierung ist die Aufhebung der →Personenbezogenheit von Daten zu einer Person. „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." [→BDSG § 3 (6)].

Erläuterung: Anonymisierung bedingt, dass eine Zuordnung der Daten zu einer Person technisch und inhaltlich nicht mehr möglich ist oder aber eine →Reidentifizierung inhaltlich nur noch mit unverhältnismäßig großem Aufwand möglich wäre, so dass ein Erfolg höchst unwahrscheinlich erscheint.

Hiervon abgeleitet kann man, je nach theoretischer Möglichkeit der →Reidentifizierung, zwischen absoluter (vollkommener) und faktischer Anonymisierung unterscheiden.

Absolute Anonymisierung liegt vor, wenn eine nicht nur technisch, sondern auch inhaltlich absolut irreversible Abtrennung der →Personenbezogenheit besteht, d.h., wenn auch theoretisch aus dem Inhalt der Daten nicht mehr auf eine Person zurückgeschlossen werden kann.

Faktische Anonymität besteht dann, wenn diese Möglichkeit des Rückschlusses bei bestimmten Datenkonstellationen (Alleinstellungsmerkmale, z.B. durch Kombination mit umfangreichen externen Datensätzen) theoretisch nicht ausgeschlossen erscheint, aber praktisch mit so hohem Aufwand verbunden wäre, dass sie unverhältnismäßig und unwahrscheinlich erscheint.

Erscheint diese →Reidentifizierung aus dem Inhalt der Daten heraus jedoch möglich, so ist die formal vollzogene Anonymisierung unvollständig und es herrscht wieder Personenbezogenheit. Als formale Anonymisierung bezeichnet man den Anonymisierungsvorgang, unabhängig davon, ob faktische oder absolute Anonymität erreicht wird oder nicht.

Gegensatz: →Personenbezogenheit.

Verwandte Begriffe: →Pseudonymisierung, eine eingeschränkte Form der Anonymisierung; faktische Anonymisierung siehe oben.

Archivierung

Definition: Dauerhafte Aufbewahrung von Daten auf geeigneten Datenträgern.

Erläuterung: Im Gegensatz zu einem Backup (Datensicherung) ist in der Regel kein online-Zugriff mehr nötig und möglich (bei elektronischer Archivierung ist der online-Zugang allerdings weiter möglich oder leicht wieder herzustellen); auch werden archivierte Daten nicht mehr geändert. Im Kontext der →medizinischen Forschungsverbünde ist die Archivierung beispielsweise für →klinische (→AMG), oder auch epidemiologische Studien relevant, wobei mindestens der Stand zum Zeitpunkt der Auswertung eingefroren werden soll. Bei Veröffentlichungen sind die Empfehlungen zur →Guten Wissenschaftlichen Praxis zu berücksichtigen.

Arzneimittelgesetz (AMG)

Definition: Das Arzneimittelgesetz (Gesetz über den Verkehr mit Arzneimitteln, AMG) ist in Deutschland ein Gesetz des besonderen Verwaltungsrechts zur Ein- und Ausfuhr von und zum Verkehr mit Arzneimitteln. „Es ist der Zweck dieses Gesetzes, im Interesse einer ordnungsgemäßen Arzneimittelversorgung von Mensch und Tier für die Sicherheit im Verkehr mit Arzneimitteln, insbesondere für die Qualität, Wirksamkeit und Unbedenklichkeit der Arzneimittel [...] zu sorgen."

Erläuterung: Das Arzneimittelgesetz dient als gesetzliche Grundlage dem Schutz der Gesundheit der Bevölkerung insbesondere durch die hohen Anforderungen an die Sorgfalt im Umgang mit Arzneimitteln durch die Pharmaindustrie, Apotheker und Ärzte. Dies betrifft vor allem die Belange: Herstellung, Inverkehrbringung, Prüfung, Verschreibung, Aufklärung und Abgabe von Arzneimitteln. Verstöße gegen das AMG werden teils als Ordnungswidrigkeiten, teils als Straf-

taten geahndet (s. §§ 95ff.).[40] Das AMG stellt strikte, auch datenschutzrechtlich relevante Anforderungen an die Durchführung einer →klinischen Studie.

Hinweis: In Österreich ist das dortige Arzneimittelgesetz, in der Schweiz das Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz) einschlägig.

Verweis: http://bundesrecht.juris.de/amg_1976/

Ärztliche Schweigepflicht

→Schweigepflicht.

Audit

Definition: Als Audit werden allgemein Untersuchungsverfahren bezeichnet, die dazu dienen, Prozessabläufe hinsichtlich der Erfüllung von Anforderungen und Richtlinien zu bewerten.[41]

Erläuterung: Die Audits werden von einem speziell hierfür geschulten Auditor durchgeführt. Im Kontext von →klinischen Studien ist ein Audit Bestandteil der →Qualitätssicherung. Hierbei werden sämtliche Prozesse auf Übereinstimmung mit Studienplan, Richtlinien, →SOPs und anderen verbindlichen Festlegungen – auch hinsichtlich Datenschutzmaßnahmen – geprüft. Ein Zugriff auf konkrete Daten ist allenfalls stichprobenartig nötig; ein Personenbezug muss im Regelfall nicht offenbart werden.

Hinweis: Auch im direkten Kontext des Datenschutzes wird der Begriff verwendet: Das Datenschutz-Audit ist im →BDSG § 9a definiert: „Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen.“ Ein solches Datenschutz-Audit wird u.a. vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) angeboten.

Aufklärung

siehe →Patienteninformation.

Auskunftsrecht

Definition: →BDSG § 19: „Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

40 vergl. http://de.wikipedia.org/wiki/Arzneimittelgesetz_%28Deutschland%29 (Abruf: 2014-08-27)
41 vergl. http://de.wikipedia.org/wiki/Audit (Abruf: 2014-08-27)

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung."

Im Datenschutzrecht besteht also das aus dem →informationellen Selbstbestimmungsrecht abgeleitete Recht, Auskunft über alle gespeicherten personenbezogenen Daten zu erlangen. Im Arztrecht besteht das Recht des Patienten, Einsicht in die objektiven Teile der ärztlichen Aufzeichnungen zu nehmen (mit wenigen Ausnahmen).

Erläuterung: Der Patient oder Proband hat das Recht, Auskunft über die Daten zu verlangen, die über ihn im Bereich des →Forschungsverbunds gespeichert werden. In der Regel wendet er sich dazu an den aktuell behandelnden Arzt, der mit dem Forschungsverbund in Verbindung steht. Der Arzt leitet dann die Prozesse ein, die zur gewünschten Auskunft führen.

Hinweise: Es ist zwischen dem datenschutzrechtlichem Auskunftsrecht und der Auskunft über Untersuchungs- oder Analyse-Ergebnisse aus einem Forschungsprojekt zu unterscheiden.

Grundlage für das datenschutzrechtliche Auskunftsrecht ist das Datenschutzrecht sowie im →Behandlungszusammenhang das Arztrecht. Das Auskunftsrecht richtet sich an den →Träger des Forschungsverbundes (oder der Biomaterialbank, der Studie, …) und wird an den in der →Einwilligungserklärung genannten Ansprechpartner gerichtet; das kann, muss aber nicht, der behandelnde Arzt sein. Es betrifft die Speicherung von →personenbezogenen Daten. In der Regel sind in einem Forschungsverbund nur bei der Datenquelle (behandelnde Einrichtung) und beim ID-Management (→Patientenliste) personenbezogene Daten gespeichert. Ergebnis eines Auskunftsgesuchs sind die genannten personenbezogenen Daten, wobei die behandelnde Stelle nach dem Arztrecht in Ausnahmefällen aus Fürsorge für den Patienten Informationen zurückhalten darf.

Für die Auskunft über Untersuchungs- oder Analyse-Ergebnisse aus einem Forschungsprojekt besteht dagegen keine Rechtspflicht. Grundlage ist die Regelung in der →Einwilligungserklärung. Hier kann eine Mitteilung auf Verlangen oder aber eine „automatische" Mitteilung vereinbart sein (oder auch das →Recht auf Nichtwissen). Falls eine Mitteilung erfolgt, darf diese nur über den behandelnden Arzt (oder einen anderen in der Einwilligungserklärung genannten Arzt) erfolgen, gegebenenfalls unter Hinzuziehung eines fachlich kompetenten Kollegen (→Konsiliarius, z.B. für die Interpretation von Bilddaten und →Befunden) sowie bei genetischen Analysen eines Humangenetikers.

Ausschuss Datenschutz

Definition: Der Ausschuss Datenschutz ist ein Gremium eines →Forschungsverbundes, das die Regelung aller mit dem Datenaustausch und dem Datenzugang zusammenhängenden Fragen verantwortet.

Erläuterung: Diesem Ausschuss kommen folgende fachlichen Aufgaben zu:

- Bewertung und Bewilligung der Anträge von Wissenschaftlern auf die Bereitstellung von Forschungsdaten, welche Ziel, Weg und Datenbedarf darstellen. Mit der Bewilligung ist zu definieren
  - der auf die Forschungsaufgabe zugeschnittene Datensatz,
  - die anzuwendenden Selektionsfilter,
  - der Zugang zu →pseudonymisierten oder →anonymisierten Daten.
- Bewertung und Bewilligung von Anträgen auf Übermittlung von Forschungsergebnissen an Patienten durch deren behandelnde Ärzte.
- Die Beauftragung der zentralen Dienste und die Verabschiedung der →Policies und Nutzungsordnungen für diese zentralen Dienste, welche die für Datenschutz und Datensicherheit relevanten Regeln enthalten.

Der Ausschuss Datenschutz kann auch durch ein Gremium verkörpert werden, das andere Aufgaben hat (und anders bezeichnet wird), z.B. durch den Vorstand. Der Datenschutzbeauftragte des Forschungsverbunds soll diesem Gremium angehören; seine vom Datenschutzgesetz definierten Rechte und Pflichten sind dadurch unberührt. Die Aufgaben des Ausschusses Datenschutz gehen über die gesetzlich definierten Aufgaben des Datenschutzbeauftragten hinaus.

BDSG

→Bundesdatenschutzgesetz.

Befund

Definition: Der medizinische Befund kann sich entweder auf die Gesamtheit der durch Ärzte erhobenen körperlichen und psychischen Erscheinungen eines →Patienten oder auf einzelne, erwartete oder unerwartete, Beobachtungs- oder Untersuchungsergebnisse beziehen. Einzelnen Befunden (→Finding) kann eine pathologische Konnotation anhaften. Die Feststellung „ohne Befund" bringt dann das Fehlen eines Hinweises auf eine Krankheit zum Ausdruck.

Behandlungszusammenhang (Behandlungskontext)

Definition: Daten und Proben werden im Behandlungszusammenhang gewonnen, wenn sie im Rahmen der Behandlung eines Patienten von einem Arzt oder dem Mitarbeiter einer Klinik oder sonstigen klinischen Einrichtung erhoben werden und ihre Zweckbestimmung in der Analyse für Zwecke der weiteren Behandlung des Patienten zu sehen ist. Daten und Proben aus dem Behandlungszusammenhang sind durch die ärztliche →Schweigepflicht besonders geschützt, solange sie diesen nicht verlassen.

Erläuterung: Sollen Daten oder Proben aus dem Behandlungszusammenhang auch für weitergehende Forschungszwecke verwendet werden, ist vor der Er-

hebung im Regelfall eine zusätzliche Information des Patienten über diese Zwecke sowie seine entsprechende →Einwilligung erforderlich.

Abzugrenzen von den im Behandlungszusammenhang gewonnenen Daten und Proben sind solche, die im →Forschungszusammenhang erhoben werden. Die Prozesse in einem medizinischen Forschungsverbund können zum Behandlungszusammenhang oder zum Forschungszusammenhang gehören. Falls hier ein Behandlungszusammenhang besteht, gilt dieser bei chronischen Erkrankungen als gewahrt, sofern der Patient spätestens alle 6 Jahre wieder bei einem behandelnden Arzt vorstellig wird und Daten zu ihm im Behandlungszusammenhang erfasst werden. Während dieser Zeit ist ein Zugriff auf die früheren Daten durch die behandelnden Ärzte möglich. Einschränkungen zu dieser Richtzeit gelten für nur mittelbar im Behandlungszusammenhang beteiligte Ärzte wie z.B. Laborärzte. Für diese werden je nach Aufgabe unterschiedliche spezifische Einschränkungen (Rollen) in dem Forschungsvorhaben definiert, vom →Ausschuss Datenschutz des Forschungsverbundes festgelegt und durch die Systembetreuer im Zugriffskonzept abgebildet.

Für nicht chronische Krankheiten ist der zur Wahrung des Behandlungszusammenhangs zureichende Zeitraum spezifisch und auch abhängig von der Forschungsmethodik im Forschungsvorhaben zu definieren.

Benchmarking

Definition: Behandlerübergreifender Vergleichsprozess zu Behandlungsabläufen und -erfolgen.

Erläuterung: Beim Benchmarking werden von mehreren Behandlern auf freiwilliger Basis Daten zum Behandlungsablauf und -ergebnis zusammengeführt und ausgewertet. Die Ergebnisse werden dem einzelnen Behandler im Regelfall so zurückübermittelt, dass ihm eine Einschätzung der von ihm erreichten Behandlungsqualität im Verhältnis zu allen anderen teilnehmenden Behandlern möglich wird. Ziel ist eine Sicherung oder Steigerung der Behandlungsqualität bei allen teilnehmenden Behandlern. Während die hierfür benötigten Patientendaten häufig →anonymisiert verglichen werden können, werden die Arztdaten (→ADAT) in →pseudonymisierter Form genutzt. Ebenfalls möglich ist eine Kopplung mit einer →Klinischen Datenbank, wobei eine zentrale Speicherung pseudonymisierter Patientendaten zum Zwecke der Qualitätssicherung eine Einwilligung voraussetzt.

Beobachtungsstudie

Definition: Bei einer Beobachtungsstudie wird (im Gegensatz zu einer →Interventionsstudie) kein gezielter Einfluss auf den Ablauf ausgeübt. Die Auswertung ist im Allgemeinen nur deskriptiv.

Erläuterung: Beobachtungsstudien dienen auch zur Hypothesenbildung für künftige →kontrollierte Studien. Die Daten aus Beobachtungsstudien können in einer →Klinischen Datenbank zusammengeführt werden (z.B. bei Langzeitbeobachtung von chronischen oder angeborenen Erkrankungen).

Beschlagnahmefestigkeit

Definition: Beschlagnahmefestigkeit ist der durch Rechtsvorschriften konstituierte Schutz von Gegenständen (Sachen, Akten, Unterlagen, Daten usw.) gegenüber beweissichernden Maßnahmen der Strafverfolgungsbehörden.

Erläuterung: Beschlagnahmeverbote ergeben sich aus verschiedenen Prozessordnungen, insbesondere aus § 97 Abs. 1 StPO. Im Unterschied zu personenbezogenen Unterlagen bei Rechtsanwälten, Notaren und Ärzten unterliegen Forschungsdaten und Proben keinem solchen Beschlagnahmeschutz. Das gilt somit auch für Daten und Proben von →medizinischen Forschungsverbünden, sobald sie den Behandlungszusammenhang verlassen.

Verweis: Zum Thema Beschlagnahmefestigkeit und Forschungsgeheimnis vgl. auch [23, S. 190ff] und [20].

BildDAT

Definition: Bilder aus bildgebenden Verfahren der Medizin, die in digitaler Form vorliegen und mit organisatorischen oder technischen Begleitdaten (→OrgDAT) versehen sind.

Erläuterung: Beispiele für solche Bilder sind

- Fotografien,
- Schnittbilder aus der Pathologie,
- endoskopische Aufnahmen,
- Röntgenbilder,
- Computer-Tomogramme (CT),
- Kernspin-Tomogramme (MRT = Magnet-Resonanz-Tomogramm),
- Nuklearmedizinische Verfahren (PET = Positron-Elektron-Tomogramm u.a.),
- Ultraschallaufnahmen (Sonogramm).

Dabei kann es sich um Einzelbilder, zusammengehörige Bilderserien oder Filme handeln. Die Bilder dienen meist zu diagnostischen Zwecken, können aber auch für die Therapieplanung benötigt werden.

Analysedaten aus Bildern (→Befunde) werden in der Regel den →MDAT zugeschlagen, da sie – im Gegensatz zu Probenanalysedaten (→ProbDAT) – kein →Reidentifizierungspotenzial besitzen. Im Gegensatz dazu haben die Bilder selbst gelegentlich (z.B. bei Fotografien) ein →Reidentifizierungspotenzial, welches im Einzelfall beurteilt und berücksichtigt werden muss.

Bilddatenbank

Definition: Eine Bilddatenbank ist eine Einrichtung, die medizinische Bilder (→BildDAT) sammelt, ggf. aufbereitet, ggf. durch demographische und krankheits- bzw. fragestellungsbezogene („medizinische", →MDAT) Daten des Probanden ergänzt und Bilder sowie evtl. Daten in geeigneter Form für Forschungszwecke zur Verfügung stellt.

Erläuterung: Eine solche Bilddatenbank stellt Referenzmaterial für Versorgung, Forschung und Lehre zur Verfügung. Wichtig dafür ist die Aufbereitung für eine effiziente Suche, z.B. nach diagnostischen Details. Verwendete Bildformate sind →DICOM sowie die im Internet gebräuchlichen Formate (z.B. JPEG).

Biobank (Biomaterialbank, Probenbank, Gewebebank, Genbank, Probensammlung)

Definition: Eine Biobank ist eine Einrichtung, die →Proben menschlicher Körpersubstanzen sammelt, ggf. aufbereitet, durch demographische und krankheits- bzw. fragestellungsbezogene („medizinische") Daten des Probanden ergänzt und Proben und Daten in geeigneter Form für Forschungszwecke zur Verfügung stellt.

Erläuterung: Eine Biobank sammelt →Proben menschlicher Körpersubstanzen (Zellen, Gewebe, Blut, ganze Organe usw.) extrahiert ggf. Anteile solcher Substanzen (etwa Serum oder DNA), ergänzt diese durch Daten des Probanden (personenbezogen, krankheitsbezogen) und stellt Proben und Daten in geeigneter Form für Forschungszwecke zur Verfügung. Die Bereithaltung der Biomaterialien und der dafür erforderlichen Daten erfolgt in der „Probenbank"; die Daten des Probanden einschließlich ermittelter Analyseergebnisse werden in „Datenbanken" abgelegt. Wichtig ist dabei die begriffliche Unterscheidung zwischen der Biobank als Gesamteinrichtung und der Probenbank als Bestandteil der Biobank, die lediglich die Sammlung der Biomaterialien darstellt. Weiterhin handelt es sich bei einer Biobank weder um ein reines Biomateriallager noch um eine reine Datenbank, sondern vielmehr um die Einheit von Biomaterial und Daten.

Eine Biobank ist auch von solchen Probensammlungen zu unterscheiden, die im Rahmen der Krankenversorgung entstehen und nur intern (etwa in einer Universitätsklinik) zur behandlungsnahen Forschung genutzt werden, ohne dass die Proben oder entsprechende Analyseergebnisse dauerhaft für weitergehende Forschungszwecke zur Verfügung gestellt werden. Probensammlungen, deren Aufbau nur inhaltlich und zeitlich befristeten Forschungsprojekten dient, werden ebenfalls nicht als Biobank im hier maßgeblichen Sinn bezeichnet.

Verweis: Grundlegend zum Begriff der Biobank im hier dargestellten Sinn auch [2] sowie [14 S. 12ff].

Biomaterial

siehe →Probe.

Biomaterialbank

siehe →Biobank.

Bundesdatenschutzgesetz (BDSG)

Definition: Setzt das vom Bundesverfassungsgericht 1983 festgestellte →informationelle Selbstbestimmungsrecht um, in dem es den Umgang mit →personenbezogenen Daten subsidiär (nachgeordnet zu anderen Gesetzen) für öffentliche Einrichtungen des Bundes, alle nicht-öffentlichen Einrichtungen und in bestimmten Fällen auch für öffentliche Einrichtungen der Länder regelt. Zudem wird die Datenschutzaufsicht für die öffentlichen Einrichtungen des Bundes geregelt.

Erläuterung: Das BDSG legt insbesondere fest, dass eine Verarbeitung und Nutzung personenbezogener Daten im Regelfall nur erfolgen darf, wenn ein Gesetz dies erlaubt oder der Betroffene eingewilligt hat. Analoge Regelungen enthalten die →Landesdatenschutzgesetze für ihren jeweiligen Anwendungsbereich.

Verweis: http://www.gesetze-im-internet.de/bdsg_1990

Case Report Form (CRF)

siehe →Dokumentationsbogen

Cloud (Cloud-Computing)

Definition: Virtualisiertes Angebot von IT-Services. Dabei können Hardwareressourcen, im wesentlichen Rechenkapazität und Speicherplatz (Infrastructure as a Service – IaaS), Anwendungs- und Entwicklungsplattformen (Platform as as Service – PaaS) als auch fertige Anwendungen (Software as a Service – SaaS) über Netzwerkverbindungen angeboten werden.

Erläuterung: Eine wichtige Unterscheidung von Cloud-Angeboten betrifft die Art des Netzwerks, über das die verschiedenen Dienste angeboten werden. Wenn dies ein öffentliches Netz ist – im Regelfall das Internet – wird von einer Public Cloud gesprochen, anderenfalls von einer Private Cloud. Nach einer alternativen Definition spricht man von einer Public Cloud, wenn der Nutzer und der Anbieter der Cloud unterschiedlichen juristischen Personen zuzuordnen sind. Dementsprechend ist dann von einer Private Cloud auszugehen, wenn der Anbieter zur selben juristischen Person gehört wie der Nutzer als datenschutzrechtlich verantwortliche Stelle für die Datenverarbeitung.

Die wesentlichen Vorteile des Cloud-Computings, die flexible und skalierbare Nutzung von Ressourcen wie Rechenleistung und Speicherplatz, verbunden

mit einer Kostenumverteilung von Investitions- zu Betriebsaufwänden, sind in ähnlicher Form auch schon für das →Grid-Computing reklamiert worden. Im Idealfall führt eine zielgenaue Mittelallokation zu einer Kostensenkung.

Verweise: Ausführliche Informationen zum Cloud-Computing aus datenschutzrechtlicher Sicht finden sich in [28] und [42], jedoch ohne näheren Bezug zum Bereich der medizinischen Forschung. Für eine Abgrenzung zum →Grid-Computing siehe [43].

Codierung

siehe →Pseudonymisierung.

Contract Research Organisation (CRO)

Definition: Auftragsforschungsinstitute übernehmen im Auftrag von →Sponsoren →klinischer Studien Teile der Studiendurchführung. Sie sind meist kommerziell ausgerichtet.

Controller

Definition: Mit der EU-Datenschutzrichtlinie 95/46/EG eingeführter Begriff für die für die Verarbeitung →personenbezogener Daten verantwortliche Stelle.

Verweis: →Datenverarbeitende Stelle

CRF

Case Report Form, siehe →Dokumentationsbogen

CRO

siehe →Contract Research Organisation

Data Warehouse

Definition: Datenbank, in der Daten aus unterschiedlichen Quellen in einem einheitlichen Format für übergreifende Auswertungen zusammengefasst werden. Daten werden hierfür aus den Quellsystemen extrahiert (Extract), so transformiert (Transform) dass ein einheitliches Format erreicht wird und schließlich in das Data Warehouse geladen (Load). Dieser Prozess wird entsprechend der drei Stufen auch ETL-Prozess genannt.

Erläuterung: Daten aus verschiedenen klinischen Dokumentationssystemen können mit Hilfe eines Data Warehouse für Forschungsfragestellungen zugänglich gemacht werden, z.B. für Rekrutierungsanfragen oder für die Abschätzung der Machbarkeit (Feasibility) einer Studie.

Datenkategorien in einem medizinischen Forschungsverbund

In einem Forschungsverbund fallen unterschiedliche Datenkategorien an. Im Einzelnen werden gemäß diesem Leitfaden zum Datenschutz folgende logische Datenkategorien unterschieden: →IDAT, →LabID, →MDAT, →BildDAT, →OrgDAT, →PID, →ProbDAT und →PSN.

Datenmanager (Datenkoordinator)

Definition: Datenmanager sind für die technischen Prozesse der Datenerfassung und -verarbeitung sowie ggf. auch für die Archivierung in klinischen Forschungsprojekten zuständig.

Erläuterung: Übliche Aufgaben eines Datenmanagers im Rahmen →klinischer Studien sind

- Erstellung von →Dokumentationsbögen (Papier oder elektronisch) entsprechend dem Studienprotokoll,
- Anwenderschulung für die Prüfzentren,
- Installation und Konfiguration der Datenerfassungssoftware,
- Festlegung der Richtlinien für die Datenerfassung, Mitwirkung bei der →SOP-Erstellung,
- Einrichtung der →Studiendatenbank,
- Logistik der Datenerfassung,
- Erstellung von Plausibilitätsprüfungen und Datenvalidierung,
- Rückfragen an Prüfzentren,
- Unterstützung von Validierungs-, Review- und →Monitoring-Prozessen,
- Bereitstellung von Daten für Auswertungen und Einreichungen bei Behörden.

Oft sind Datenmanager auch mit dem technischen Support der eingesetzten Software oder mit der statistischen Auswertung der Daten beauftragt.

Verweis: Weitere Informationen finden sich in [44].

Datenqualität

Definition: Grad, in dem eine Menge von Daten Anforderungen, z.B. hinsichtlich Genauigkeit, Vollständigkeit und Korrektheit, erfüllt.

Erläuterung: Unter Qualitätsmanagement versteht man aufeinander abgestimmte Tätigkeiten zum Leiten und Lenken einer Organisation bezüglich ihrer Qualität. Dazu gehören üblicherweise das Festlegen der Qualitätspolitik und der Qualitätsziele, die Qualitätsplanung, die Qualitätslenkung, die Qualitätssicherung und die Qualitätsverbesserung. Qualitätssicherung ist ein Teil des Qualitätsmanagements mit dem Ziel, Vertrauen dahingehend zu erzeugen, dass Qualitätsanforderungen erfüllt werden.

In der Regel sind Datenerhebungen in →medizinischen Forschungsverbünden mit einer oder mehreren Stufen der Qualitätssicherung verbunden; Umfang und Komplexität der Qualitätssicherung sind durch das Studiendesign und die Normen, denen es sich unterwirft, definiert. Immer geht es dabei um die Ergänzung und Korrektur fehlender, unvollständiger und implausibler Daten. Bei →epidemiologischen Studien setzen die Forscher selbst die Anforderungen und Verfahren fest. Bei →klinischen Studien sind die Anforderungen durch →„Standard Operation Procedures“ von außen festgelegt.

Verweis: Weitere Informationen in [45].

Datentreuhänder

Definition: Der Datentreuhänder ist eine rechtlich, räumlich und personell selbstständige und unabhängige Stelle, die idealerweise einer besonderen Geheimhaltungspflicht unterliegt, z.B. ein Notar oder ein externer Arzt.

Erläuterung: Der Datentreuhänder tritt zwischen eine Forschungsdaten besitzende Stelle und den Forscher und sichert dadurch die Rechte der betroffenden →Patienten und Probanden. Er →anonymisiert oder →pseudonymisiert die von der Daten besitzenden Stelle übermittelten →personenbezogenen Daten und übermittelt nur die anonymisierten bzw. pseudonymisierten Daten an den Forscher weiter. Auf diese Weise bleibt der Kreis derjenigen, die Kenntnis von personenbezogenen Daten erhalten, eng begrenzt, und die Datensicherheit kann effektiv gewährleistet werden. Die durch den Datentreuhänder wahrgenommene Funktion eines „vertrauenswürdigen Dritten“ kann noch verstärkt werden, wenn dieser einer Berufsgruppe angehört, die gesetzlich zur Verschwiegenheit verpflichtet ist und deren Unterlagen und Daten u.U. einem →Beschlagnahmeschutz unterliegen (Beispiele: Rechtsanwälte, Notare).

Datentreuhänder werden bereits von einigen medizinischen Kompetenznetzen eingesetzt (beispielhaft: Kompetenznetz Parkinson e.V.).

Verweis: Näheres zur Rolle und den Aufgaben eines Datentreuhänders findet sich bei Metschke und Wellbrock [19 S. 41ff] und Dierks [20]

Datenverarbeitende Stelle

Die für die Verarbeitung personenbezogener Daten verantwortliche Stelle.

→Controller

Depseudonymisierung

Definition: Befugte Wiederherstellung des →Personenbezugs von pseudonymisierten Daten und Proben.

Erläuterung: Dies wird durch Umkehrung des →Pseudonymisierungsverfahrens erreicht. Despeudonymisierung wird in bestimmten Anwendungsfällen als kontrollierter Vorgang aktiv betrieben, z.B. bei der Rückübermittlung von Forschungserkenntnissen an einen Patienten, die auf der Basis pseudonymisierter Daten gewonnen wurden. Davon zu unterscheiden ist die →Reidentifizierung als unbefugte Wiederherstellung des Personenbezugs.

Verwandte Begriffe: →Anonymisierung und →Pseudonymisierung.

DICOM

Definition: Digital Imaging and Communications in Medicine. DICOM ist ein weltweit offener Standard zum Austausch von digitalen Bildern in der Medizin.

Erläuterung: DICOM standardisiert sowohl das Format zur Speicherung von Bilddaten als auch das Kommunikationsprotokoll zum Austausch der Bilder. Fast alle Hersteller medizinisch bildgebender Systeme wie z.B. Digitales Röntgen, Magnetresonanztomographie, Computertomographie oder Sonografie implementieren den DICOM-Standard in diesen Geräten. Dadurch wird im klinischen Umfeld Interoperabilität zwischen medizinischen Systemen verschiedener Hersteller erreicht. DICOM beinhaltet neben Datenfeldern (z.B. Informationen über Bilder, →Befunde, →Patienten, →Studien, Serien, …) auch die Syntax und Semantik von Kommandos und Nachrichten. Weiterhin legt der Standard Vorschriften für die Beschreibung von DICOM-kompatiblen Geräten und Software fest, da für jedes DICOM-kompatible Gerät eine exakte Beschreibung der Systemfähigkeit vorhanden und veröffentlicht sein muss (DICOM Conformance Statement). Ein DICOM-Datensatz dient als Container. Er enthält außer einem oder mehreren Bildern auch Metainformationen wie Patientenname, Aufnahmedatum, Geräteparameter oder Arztname.[42]

Dokumentationsbogen

Definition: Auf Papier oder elektronisch bereit gestelltes Formular zur Datenerfassung in klinischen Forschungsprojekten.

Verweis: s.a. →Datenmanager

EDC

Electronic Data Capture, siehe →Remote Data Entry

EFA

→Elektronische Fallakte

42 vergl. http://de.wikipedia.org/wiki/Dicom (Abruf: 2014-08-27)

EGA

→Elektronische Gesundheitsakte

Einwilligungserklärung (informed consent, Einwilligung nach Aufklärung, Einverständniserklärung)

Definition: Die vom Datenschutzrecht geforderte Voraussetzung zur Verarbeitung →personenbezogener Daten des Betroffenen, sofern diese nicht aufgrund eines Gesetzes erlaubt ist.

Erläuterung: Die Einwilligungserklärung eines →Patienten oder Probanden ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist zuvor über den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung seiner Daten und →Proben aufzuklären („informed consent"). Die Wirksamkeit der Einwilligungserklärung erfordert deren Schriftform. Soll sie zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Materiellrechtlich setzt die Einwilligungserklärung die Einsichtsfähigkeit des Erklärenden voraus.

Hinweise: Der oft gebrauchte Begriff „Einverständniserklärung" sollte im Kontext der medizinischen Behandlung oder Forschung nicht gebraucht werden, da er die Manifestation des Willens des Betroffenen nicht deutlich ausdrückt.

Im Behandlungszusammenhang gilt die vereinfachte Regelung des Arztrechts. Im Rahmen der Zweckbestimmung des Behandlungsvertrages ist das Speichern und Verabreiten von Patientendaten ohne explizite Einwilligung erlaubt. Man spricht von konkludenter Einwilligung, die sich aus dem Wunsch des Patienten nach sachgerechter Behandlung ergibt.

Verweis: Zu den gesetzlichen Anforderungen an die Einwilligungserklärung siehe § 4a Abs. 1 →BDSG; siehe dort auch den Sonderfall in § 4a Abs. 2 BDSG, wenn im Bereich der wissenschaftlichen Forschung durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde; in einem solchen Fall kann u.U. auf das Erfordernis der Schriftlichkeit verzichtet werden.

Elektronische Fallakte (EFA)

Definition: Elektronische Fallakten sind eine – ggf. nur virtuelle – einrichtungsübergreifende Zusammenführung behandlungsrelevanter Unterlagen zu einem →Behandlungsfall zur Unterstützung der intersektoralen Kooperation. Der Zweck der Datenverarbeitung ist der konkrete Behandlungsfall, das Ziel eine bessere Informierung der verschiedenen beteiligten ärztlichen Akteure. Im Regelfall bildet eine informierte →Einwilligung der Patienten die Rechtsgrundlage.

Elektronische Gesundheitsakte (EGA)

Definition: In einer Elektronischen Gesundheitsakte werden einrichtungsübergreifend und behandlungsfallübergreifend gesundheitsrelevante Informationen zu einem Patienten oder auch gesunden Bürger gespeichert und verarbeitet. Da die Datenhaltung in einer EGA weniger eindeutig zweckbezogen erfolgt als in einer →Elektronischen Fallakte, ist nicht nur eine informierte →Einwilligung des Betroffenen sondern darüber hinaus auch seine stärkere Einbindung in die Führung und Steuerung der EGA notwendig, bis hin zur eigenen Beisteuerung von Informationen.

Erläuterung: Eine beispielhafte Regelung für eine EGA findet sich im Kontext der gesetzlichen Grundlagen der elektronischen Gesundheitskarte in § 291a SGB V, dort als Elektronische Patientenakte (EPA) aufgeführt.

EPA

Elektronische Patientenakte, siehe →Elektronische Gesundheitsakte

Epidemiologie

Definition: Die Epidemiologie ist ein medizinisches Fachgebiet, das sich mit den Ursachen und Folgen sowie der Verbreitung von gesundheitsbezogenen Einflüssen und Ereignissen in einer Bevölkerung beschäftigt.[43] Die Epidemiologie untersucht somit jene Faktoren, die zu Gesundheit und Krankheit von Individuen und Populationen beitragen und ist deshalb die Basis aller Maßnahmen, die im Interesse der Volksgesundheit unternommen werden.

Verweis: siehe →epidemiologische Studie.

Epidemiologische Studie

Definition: Eine Studie, bei der Fragestellungen der →Epidemiologie bearbeitet werden.

Erläuterung: Die wichtigsten Studientypen sind

- →Querschnittstudien,
- →Längsschnittstudien,
- →Kohortenstudien,
- →Fall-Kontroll-Studien,
- →Interventionsstudien.

Verweis: Leitlinien und Empfehlungen zur Guten Epidemiologischen Praxis der Deutschen Gesellschaft für Epidemiologie (DGEpi) [13]

43 vergl. http://de.wikipedia.org/wiki/Epidemiologie (Abruf: 2014-08-27)

Ethik-Kommission

Definition: →GCP-V § 3 (2c): „Ethik-Kommission ist ein unabhängiges Gremium aus im Gesundheitswesen und in nichtmedizinischen Bereichen tätigen Personen, dessen Aufgabe es ist, den Schutz der Rechte, die Sicherheit und das Wohlergehen von betroffenen Personen … zu sichern und diesbezüglich Vertrauen der Öffentlichkeit zu schaffen, indem es unter anderem zu dem Prüfplan, der Eignung der Prüfer und der Angemessenheit der Einrichtungen sowie zu den Methoden, die zur Unterrichtung der betroffenen Personen und zur Erlangung ihrer Einwilligung nach Aufklärung benutzt werden und zu dem dabei verwendeten Informationsmaterial Stellung nimmt."

Erläuterung: „Der →Sponsor reicht in schriftlicher Form … bei der zuständigen Ethik-Kommission einen Antrag auf zustimmende Bewertung der →klinischen Prüfung ein." [→GCP-V § 7 (1)]. Zudem gibt es im Arztrecht eine Pflicht, sich im Vorfeld eines Forschungsprojekts von einer Ethik-Kommission beraten zu lassen.

Fall-Kontroll-Studie (FK-Studie)

Definition: Eine Fall-Kontroll-Studie ist eine Form der →epidemiologischen Studie. Es handelt sich um eine retrospektive Untersuchung von einer Stichprobe, die aus erkrankten Personen besteht (Fälle) und einer Stichprobe, die aus gesunden Personen besteht (Kontrollen).[44]

Erläuterung: Eine Fall-Kontroll-Studie geht methodisch den umgekehrten Weg einer →Kohortenstudie. Bei einer Fall-Kontroll-Studie ist der Krankheitsstatus bekannt und die Exposition (zunächst) unbekannt. Sie eignet sich insbesondere für seltene Erkrankungen, da eine Kohortenstudie sehr viele Teilnehmer haben müsste, um eine statistisch ausreichende Anzahl Erkrankter zu erreichen. Die Studienpopulation der Fall-Kontroll-Studie besteht aus einer Fallgruppe und einer →Kontrollgruppe. Erst nach der Zuordnung zu den beiden Gruppen wird die Exposition erfasst, um Beeinflussungen des Ergebnisses durch die Beobachter auszuschließen.

FDB

siehe →Forschungsdatenbank

Finding

Definition: Einzelnes, erwartetes oder unerwartetes, ärztliches Beobachtungs- oder Untersuchungsergebnis (vgl. →Befund). Wenn im Rahmen eines →Forschungsvorhabens umfangreiche medizinische Daten gesammelt werden,

---

44 vergl. http://de.wikipedia.org/wiki/Fall-Kontroll-Studie (Abruf: 2014-08-27)

kann deren Auswertung z.T. auch nach Abschluss des Vorhabens zu Findings führen, über die ein →Patient ggf. zu informieren ist.

Forscher

siehe →Nutzer.

Forschungsdaten

siehe →MDAT.

Forschungsdatenbank (FDB)

Definition: Datenbank, in der medizinische Daten aus den in einem →Forschungsverbund zusammengeschlossenen medizinischen Einrichtungen und Studien langfristig gesammelt werden. Zweck ist die wissenschaftliche Auswertung, auch über längere Zeiträume hinweg. Im Gegensatz zu einer →klinischen Datenbank beschränkt sich der Bezug zum Patienten nur auf die Möglichkeit, Daten aus verschiedenen Quellen und von anderen Zeitpunkten korrekt zusammenzuführen.

Erläuterung: Eine FDB sammelt im Wesentlichen die im Forschungsverbund verfügbaren forschungsrelevanten Daten und bietet einen zeitlich und räumlich weitgehend uneingeschränkten Zugriff auf Forschungsdaten, oft sogar mit der Möglichkeit, online Recherchen, Analysen und Verknüpfungen durchzuführen. Ein unmittelbarer Einfluss der Datenzusammenführung auf klinische Prozesse wird

nicht angestrebt, so dass die Forschungsdatenbank in einem reinen →Forschungszusammenhang angesiedelt ist. Die erhobenen Daten sind auch nicht in jedem Fall im unmittelbaren Behandlungsprozess gewonnen und dort verfügbar, sondern werden auch in speziellen Erhebungen generiert.

Hinweise: Weil die Daten in der Regel nicht der klinisch motivierten Qualitätskontrolle unterliegen, ist vor der Übernahme der Informationen in die Forschungsdatenbank ein vorgeschaltetes →Qualitätssicherungssystem erforderlich, welches im Feedback zur Datenquelle Mängel in der Plausibilität und Vollständigkeit der Daten minimiert. Die Forschungsdatenbank ist der zentrale Datenpool im Modell B des bisherigen generischen Datenschutzkonzepts der TMF [1].

Forschungsnetz

siehe →Medizinischer Forschungsverbund.

Forschungsverbund (Forschungsnetz)

siehe →Medizinischer Forschungsverbund.

Forschungsvorhaben (Studie)

Definition: Medizinische Forschungsprojekte werden oft als Studien bezeichnet. Ziel einer solchen Studie sind neue Erkenntnisse über Entstehung, Verlauf, Diagnose, Behandlung von Krankheiten oder deren Langzeitauswirkungen.

Erläuterung: Ein Forschungsvorhaben kann in unterschiedlichen Formen durchgeführt werden. Am meisten verbreitet sind dabei →klinische Studien, also die wissenschaftliche Auswertung diagnostischer und therapeutischer Maßnahmen am kranken Patienten, und →epidemiologische Studien, also die bevölkerungsbezogene Untersuchung einer Erkrankung und ihrer Ursachen. Bei vielen Studien (sog. kontrollierten Studien) wird neben einer Gruppe von Patienten auch eine →Kontrollgruppe benötigt.

Hinweise: Methodische Grundlagen sind u.a. molekulargenetische Analysen und statistische Auswertungen.

Forschungszusammenhang (Forschungskontext)

Definition: Daten und Proben, mit denen →Forschungsvorhaben durchgeführt werden, stehen im Forschungszusammenhang.

Erläuterung: Sie können direkt im Forschungszusammenhang erhoben oder aus dem →Behandlungszusammenhang in den Forschungszusammenhang überführt werden. Im Forschungszusammenhang werden Daten und Proben auch erhoben, wenn zum Zeitpunkt ihrer Gewinnung bereits klar ist, dass diese unabhängig von einer konkreten Behandlung oder in Ergänzung ihrer Verwendung im →Behandlungszusammenhang in eine Datenbank für die Forschung integriert werden sollen. In diesem Fall ist der Patient oder Proband, soweit dies zum Zeitpunkt der Daten- oder Probengewinnung schon möglich ist, ausführlich über die geplante Verwendung aufzuklären, und seine schriftliche →Einwilligung ist einzuholen.

Verweise: Weitere Einzelheiten dazu auch bei den Begriffen →Patienteninformation, →Einwilligungserklärung und →Widerruf.

GCP

siehe →Good Clinical Practice.

GCP-V

siehe →GCP-Verordnung

GCP-Verordnung (GCP-V)

Definition: Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen.

Verweise: siehe auch →Good Clinical Practice, GCP-V im Internet unter http://www.gesetze-im-internet.de/gcp-v

Genbank

siehe →Biobank.

Gewebebank

siehe →Biobank.

Good Clinical Practice (GCP, Gute Klinische Praxis)

Definition: Good Clinical Practice bezeichnet nach ethischen und praktischen Gesichtspunkten aufgestellte, vom aktuellen Stand der wissenschaftlichen Erkenntnis abhängige Regeln für die Durchführung von medizinischen Behandlungen oder klinischen Tests.[45]

Erläuterung: „Der →Sponsor, der →Prüfer und alle weiteren an der →klinischen Prüfung beteiligten Personen haben bei der Durchführung der klinischen Prüfung eines Arzneimittels bei Menschen die Anforderungen der guten klinischen Praxis nach Maßgabe des Artikels 1 Abs. 3 der Richtlinie 2001/20/EG einzuhalten." [AMG § 40]

Ergänzt werden die GCP-Leitlinien durch Leitlinien für die Herstellung der eingesetzten Arzneimittel und der Medizinprodukte (GMP, Good Manufacturing Practice) sowie die im Rahmen der Studie benötigten Leistungen der Labormedizin (GLP, Gute Laborpraxis).

Organisationen, die solche Regelsätze entwerfen, sind im europäischen Raum die Europäische Arzneimittelagentur (EMEA) und international die International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH).

Verweise: http://www.ich.org/, http://www.emea.europa.eu/, →GCP-V

Grid (Grid-Computing)

Definition: Über ein Netzwerk verbundene Rechen- und Speicherressourcen, die von jedem Anschluss an das Netzwerk aus genutzt werden können. Bei Bedarf kann durch parallele Nutzung von Ressourcen deutlich mehr Speicher- oder Rechenleistung abgerufen werden als einzelne Rechenzentren typischerweise liefern.

Erläuterung: Wie beim →Cloud-Computing ist ein Hauptmotiv für die Bereitstellung und Nutzung von Grids die ökonomischere Auslastung von Hardware-

45 vergl. http://de.wikipedia.org/wiki/Good_Clinical_Practice (Abruf: 2014-08-27)

Ressourcen und die Möglichkeit, kurzfristig Ressourcen in einem Umfang zu nutzen, der bei vollständiger eigener Vorhaltung unbezahlbar wäre.

Verweis: Eine Einführung in den Aufbau einer Grid-Infrastruktur für die Forschung gibt [46]. Für eine Abgrenzung zum →Cloud-Computing siehe [43]. Sicherheits- und Datenschutzaspekte im Grid werden in [47] behandelt.

Gute wissenschaftliche Praxis

Definition: Allgemein anerkannte ethische Grundsätze, wie wissenschaftliche Vorhaben durchzuführen sind.

Erläuterung: In Deutschland vor allem definiert in den Empfehlungen der DFG-Kommission „Selbstkontrolle in der Wissenschaft.“: „Wissenschaftliche Arbeit beruht auf Grundprinzipien, die in allen Ländern und in allen wissenschaftlichen Disziplinen gleich sind. Allen voran steht die Ehrlichkeit gegenüber sich selbst und anderen.“

Verweise: http://www.dfg.de/, Leitlinien für gute epidemiologische Praxis online unter http://www.dgepi.de/doc/Empfehlungen.doc.

IDAT = Personendaten oder identifizierende Stammdaten

Definition: Personenidentifizierende Daten umfassen Name, Geburtsort, Geburtsdatum usw. des Patienten oder Probanden.

Erläuterung: Sie werden vom Arzt oder der Klinik bzw. dem Studienzentrum erhoben und je nach Organisation des Forschungsverbundes bei der erhebenden Stelle oder in einer zentralen →Patientenliste gespeichert. Es ist auch möglich, dass die IDAT bei beiden Stellen gespeichert werden.

Identitätsmanagement

siehe →Patientenliste.

IIT

siehe →Investigator Initiated Trial.

Informationelles Selbstbestimmungsrecht

siehe →Selbstbestimmungsrecht

Informed Consent

siehe →Einwilligungserklärung.

Interventionelle Studie.

siehe →Interventionsstudie.

Interventionsstudie (interventionelle Studie)

Definition: Studie, bei der zumindest bei einem Teil der Probanden ein definierter Eingriff, z.B. eine therapeutische Maßnahme, vorgenommen wird, deren Effekt untersucht werden soll.

Erläuterung: Es wird also nicht nur beobachtet, was ohne gezielte Beeinflussung ohnehin geschieht, im Gegensatz zu einer Beobachtungsstudie. Sowohl →klinische als auch →epidemiologische Studien können interventionell sein.

In der Epidemiologie verfolgt eine Interventionsstudie ähnlich einer prospektiven →Kohortenstudie eine Population entlang der Zeit, wobei man den Einfluss einer spezifischen Intervention, meist eine neue Behandlung oder ein neues Medikament, auf das Krankheitsrisiko messen möchte. Vor der Studie wird die Population in den Interventionszweig und den Kontrollzweig geteilt. Während der Studie wird dann aktiv diese Intervention (z.B. Medikament) gegeben, während die →Kontrollgruppe unbehandelt bleibt bzw. eine nichtwirksame Behandlung bekommt (z.B. Placebo).

Investigator Initiated Trial (IIT, wissenschaftsgetriebene Studie)

Definition: →Klinische Studie, der primär ein wissenschaftliches Interesse zugrunde liegt und die entsprechend im Regelfall eine akademische Einrichtung als →Sponsor hat. Abzugrenzen davon sind klinische Studien mit einem kommerziellen Interesse, z.B. im Rahmen eines Zulassungsverfahrens. Diese haben entsprechend einen Pharma- oder Medizinprodukte-Hersteller als Sponsor.

Erläuterung: Seit der 12. AMG-Novelle unterliegen IITs und kommerzielle Studien denselben gesetzlichen Anforderungen.

IT-Grundschutz

Definition: Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene Sammlung von Mindestanforderungen und entsprechenden Anleitungen zur Absicherung von Computern und Netzen.

Erläuterung: IT-Grundschutz bietet eine einfache Methode, dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Das BSI stellt zahlreiche Werkzeuge zur Verfügung, um ein angemessenes Sicherheitsniveau zu erreichen, wie z.B. die BSI-Standards zum IT-Sicherheitsmanagement, die IT-Grundschutz-Kataloge und das GSTOOL. Dazu gehört aber auch die ISO 27001-Zertifizierung auf Basis von IT-Grundschutz,

die sowohl eine Prüfung des IT-Sicherheitsmanagements als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz umfasst. Die IT-Grundschutz-Kataloge beinhalten die Baustein-, Maßnahmen- und Gefährdungskataloge.

Hinweis: Das „IT-Grundschutzhandbuch“ heißt seit der Version 2005 „IT-Grundschutz-Kataloge“.

Verweis: http://www.bsi.de/gshb/

k-Anonymität

Definition: Eine Datensammlung ist *k*-anonym, wenn die Kombination der auch in anderen Datensammlungen vorhandenen Attribute in *k* verschiedenen Datensätzen innerhalb der Datensammlung vorkommt, anders ausgedrückt, wenn es mindestens *k* Datensätze gibt, auf die das externe Wissen passt. Als andere Datensammlungen sind diejenigen zu berücksichtigen, die einem potenziellen Angreifer zum Abgleich zur Verfügung stehen könnten.

Erläuterung: Als andere Datensammlungen sind insbesondere öffentlich verfügbare oder soziodemographische Datenzusammenstellungen zu berücksichtigen. Das Grundprinzip kann auch auf pseudonymisierte Datensammlungen übertragen werden.

Klinische Datenbank

Definition: Datenbank, in der medizinische Daten aus dem Behandlungsprozess der in einem →medizinischen Forschungsverbund zusammengeschlossenen medizinischen Einrichtungen langfristig gesammelt werden. Zweck ist neben der wissenschaftlichen Auswertung auch die Verbesserung der einrichtungsübergreifenden Kooperation bei der Behandlung komplexer oder auch chronischer Erkrankungen. Im Gegensatz zu einer →Forschungsdatenbank wird ein engerer Bezug zum Patienten aufrecht erhalten.

Erläuterung: Hier steht die unmittelbare Ableitung der wissenschaftlichen Daten aus dem Behandlungsprozess im Mittelpunkt. Durch die zeitnahe Zusammenführung der Daten aus dem Behandlungsprozess für Forschungszwecke kann als Nebeneffekt die klinische Befundkommunikation verbessert werden. →Behandlungs- und →Forschungszusammenhang gehen hier ineinander über, was erhöhte Sorgfalt bei der Gestaltung von Zugriffsregelungen erfordert.

Hinweise: Die wissenschaftliche Nutzung der in einer klinischen Datenbank zusammengeführten Informationen kann, darf und soll nicht online erfolgen, sondern nur im asynchronen Zugriff auf eigens an die wissenschaftliche Fragestellung adaptierte, exportierte Teilmengen der Behandlungsdaten. Die klinischen Daten können durch die im Behandlungsprozess vorhandenen qualitätssichernden Maßnahmen überprüft werden, ein Rückgriff auf die Daten-

quelle beim Export der Forschungsdaten ist nicht notwendig. Die klinische Datenbank ist der zentrale Datenpool im bisherigen Modell A des generischen Datenschutzkonzepts.

Verwandter Begriff: →Studiendatenbank.

Klinische Prüfung

siehe →klinische Studie.

Klinische Studie (klinische Prüfung)

Definition: Eine klinische Studie dient zur Prüfung des Einflusses einer medizinischen Behandlung auf eine Krankheit unter kontrollierten Randbedingungen; Gegenstand einer klinischen Studie kann auch die Prüfung einer präventiven oder diagnostischen Maßnahme sein.

Erläuterung: Eine klinische Studie ist ein Forschungsvorhaben, bei dem der Nutzen eines präventiven, diagnostischen oder therapeutischen Verfahrens geprüft werden soll. Man unterscheidet interventionelle klinische Prüfungen (→Interventionsstudien), die einem festen Studienprotokoll folgen und oft durch das AMG (→Arzneimittelgesetz) oder MPG (→Medizinprodukte-Gesetz) geregelt sind; solche Studien können sein:

- Präventionsstudien,
- Therapievergleiche,
- →Therapieoptimierungsstudien,

sowie →nichtinterventionelle Prüfungen (sonstige Studien), die nicht dem AMG oder MPG unterliegen; dies können z.B. sein:

- Studien zur Anwendung bestimmter Produkte am Menschen (Diät-Nahrungsmittel, Hautdesinfektionsmittel, Kosmetika, Produkte zur Gesundheitsvorsorge, …),
- Evaluation diagnostischer Verfahren oder nichtmedikamentöser therapeutischer Verfahren,
- Belastbarkeits- oder Eignungsstudien.

klinischer Datenmanager (Clinical Data Manager, CDM)

siehe →Datenmanager

Kohorte (Kohortenstudie)

Definition: Eine Kohortenstudie untersucht eine definierte Gruppe von Menschen („Kohorte“) mit und ohne Exposition mit einem Risikofaktor über eine längere Zeit und misst am Ende des Beobachtungszeitraums den Erkrankungsstatus.

Erläuterung: Aus der Anzahl Erkrankter unter den Exponierten dividiert durch die Gesamtzahl an Exponierten kann das Risiko der Exponierten für diese Erkrankung gemessen werden. Analog verfährt man für die Nicht-Exponierten. Das Verhältnis des Risikos der Exponierten zum Risiko der Nicht-Exponierten ist das relative Risiko; es gibt an, wie stark die Exposition das Risiko der Erkrankung erhöht.

Konsil

Definition: Als Konsil bezeichnet man in der Medizin die patientenbezogene Beratung eines Arztes durch einen ärztlichen Kollegen, meist einen Facharzt.

Erläuterung: Der Begriff findet häufig im Krankenhaus Anwendung, wenn ein Arzt einer anderen Fachrichtung hinzugezogen wird. Der beauftragte Arzt (Konsiliarius) legt seine Empfehlungen zur Diagnostik oder Therapie meist schriftlich nieder.[46] Während der Konsiliarius in die Behandlung eingebunden ist und im Regelfall die Identität des Patienten kennt, entweder aufgrund eigener Untersuchungen oder der Vorlage entsprechender Unterlagen, wird die Referenzbefundung im Rahmen →klinischer Studien und hier insbesondere in →multizentrischen Studien im Regelfall →pseudonymisiert durchgeführt. Weitere Ausführungen bei Dierks [22].

Kontrollgruppe

Definition: Diejenigen Patienten oder Probanden, die

- bei einer →klinischen Studie nicht mit dem zu untersuchenden Therapieverfahren behandelt werden,
- bei einer epidemiologischen →Kohortenstudie nicht der zu untersuchenden Exposition ausgesetzt sind,
- bei einer epidemiologischen →Fall-Kontroll-Studie nicht das zu untersuchende Krankheitsbild entwickelt haben.

Erläuterung: Durch den Vergleich von Fall- bzw. Behandlungs- und Kontrollgruppe werden valide Aussagen über den Effekt gewonnen. Die Zuordnung zur Behandlungsgruppe und Kontrollgruppe ist der kritische Punkt einer →Interventionsstudie, da sich die Teilnehmer in ihren Gesundheitsparametern unterscheiden und man nur den Einfluss der Intervention und nicht dieser Parameter messen möchte. Erfolgt diese Auswahl zufällig und damit nicht gerichtet, spricht man von einer randomisierten, kontrollierten Studie (engl. randomised controlled trial). Diese Studien haben eine besonders starke Kausalität in Bezug auf Intervention und Krankheitsstatus und werden daher in der Medikamententestung eingesetzt. Je nach Fragestellung kann die Kontrollgruppe aus Gesunden oder Kranken bestehen.

46 vergl. http://de.wikipedia.org/wiki/Konsil (Abruf: 2014-08-27)

Kontrollierte Studie

→Forschungsvorhaben, →Kontrollgruppe.

LabID = Probennummer

Definition: Die LabID bezeichnet die ursprüngliche Nummer der Probe, die entweder von der probengewinnenden Stelle oder von der Probenbank vergeben wird.

Erläuterung: Bei der LabID kann es sich auch um einen Barcode handeln, der maschinenlesbar ist und maschinell weiterverarbeitet werden kann. Wird eine Probe aliquotiert, so können für die Teilproben zusätzliche LabIDs vergeben werden (LabID_2, LabID_3 etc.), deren Zuordnung zur LabID der Mutterprobe allerdings in der Probenbank gespeichert werden sollte. Die LabID wird entweder durch die probengewinnende Stelle oder durch das verarbeitende bzw. analysierende Labor an die zentrale Datenbank gemeldet. In der zentralen Datenbank wird statt der LabID eine transformierte (codierte, →pseudonymisierte) $LabID_{tr}$ gespeichert, um eine direkte Zuordnung von Datensatz und Probe zu vermeiden.

Landesdatenschutzgesetze (LDSG)

Definition: Regeln subsidiär (nachgeordnet zu anderen Gesetzen) den Umgang mit →personenbezogenen Daten zur Sicherung des Rechts auf →informationelle Selbstbestimmung. Anwendungsbereich sind die öffentlichen Einrichtungen der Länder. Zudem legen die LDSG die Datenschutzaufsicht für die öffentlichen Einrichtungen der Länder und die nicht-öffentlichen Einrichtungen fest.

Erläuterung: In Deutschland gibt es 16 leicht unterschiedliche LDSG.

Längsschnittstudie

Definition: Eine Längsschnittstudie erhebt regelmäßig Daten der Studienpopulation über einen längeren Zeitraum hinweg.

Erläuterung: Eine Längsschnittstudie entspricht also einer Folge von periodisch wiederholten →Querschnittstudien.

Leitlinie

siehe →Policy

Material

siehe →Probe.

MDAT = Forschungsdaten oder medizinische Daten

Definition: MDAT ist die übergreifende Bezeichnung für Daten, die zum Zwecke der Forschung in der zentralen Datenbank eines →medizinischen Forschungsverbundes gespeichert werden. MDAT umfassen in der Regel klinische Sachverhalte wie →Befunde und Diagnosen sowie soziodemographische Daten, die eine entsprechende Klassifikation des Patienten oder Probanden zu wissenschaftlichen Zwecken erlauben.

Erläuterung: Zu den soziodemographischen Daten gehören neben Alter, Geschlecht und Bildung auch Lifestylefaktoren wie etwa Ernährungsgewohnheiten sowie Umweltdaten, die eine relevante Exposition des Patienten gegenüber Klima, Luftverschmutzung oder Lärm näher charakterisieren. Mit dem medizinischen Datensatz werden auch die „sonstigen Begleitdaten" (s. →OrgDAT) gespeichert, die unter anderem das Vorliegen der Einwilligungserklärung, den Ort der Archivierung, den Umfang der Einwilligung, die Identität behandelnder Ärzte und die Daten erhebende Stelle umfassen.

Medizinischer Forschungsverbund (Medizinisches Forschungsnetz)

Definition: Ein medizinischer Forschungsverbund ist eine vernetzte Organisation mit dem Zweck, Daten oder Proben für die medizinische Forschung zu sammeln, langfristig aufzubewahren und für verschiedene, oft noch nicht feststehende wissenschaftliche Fragestellungen (→Forschungsvorhaben, Studien) auszuwerten.

Erläuterung: Der Begriff „medizinischer Forschungsverbund" wurde als Oberbegriff gewählt; er umfasst medizinische Kompetenznetze, Koordinierungszentren für klinische Studien, Biomaterialbanken und andere, meist krankheitsspezifische Forschungsnetze und Register. In vielen Fällen gibt es eine enge Verzahnung mit der medizinischen Versorgung, d.h., →Behandlungszusammenhang und →Forschungszusammenhang gehen ineinander über. In manchen Situationen, z.B. bei seltenen Erkrankungen, ist sinnvolle klinische Forschung erst durch die Vernetzung möglich. Ein Forschungsverbund kann eine lose Kooperation von Forschern verschiedener Kliniken, aber auch eine öffentlich rechtliche oder privatrechtliche Organisation sein.

Hinweise: Die TMF begreift sich als Dachverband für medizinische Forschungsverbünde; die Definition entspricht der Satzung der TMF. Siehe auch →Träger.

Medizinprodukte-Gesetz (MPG)

Definition: Das Medizinprodukte-Gesetz enthält die technischen, medizinischen und Informations-Anforderungen sowie Betreiber- und Anwendervorschriften für Medizinprodukte.

Erläuterungen: Medizinprodukte sind Instrumente, Apparate, Vorrichtungen, Stoffe oder andere Gegenstände einschließlich Software. Sie werden in vier Klassen

- I: nicht invasiv, geringes Risiko (Beispiele: Augenklappen, Thermometer),
- IIa: mittleres Risiko, kurze Anwendung (Beispiel: OP-Handschuhe),
- IIb: mittleres Risiko, Langzeitanwendung (Beispiel: Blutbeutel),
- III: hohes Risiko (Beispiel: Venenverweilkatheter)

eingeteilt.

Grundlegend für diesen Rechtsbereich ist die EU-Richtlinie 93/42/EWG. Diese Richtlinie wurde mit dem am 1. Januar 1995 in Kraft getretenen Medizinprodukte-Gesetz in deutsches Recht umgesetzt.

Verweis: http://bundesrecht.juris.de/mpg/

Medizinprodukte-Studie (MPG-Studie)

Definition: Eine solche Studie dient der Bewertung eines Medizinprodukts (z.B. Messgeräts) und hat als Ziel, die Konformität des Produkts mit den Anforderungen des Medizinprodukte-Gesetzes festzustellen; das Erreichen des Ziels wird durch ein CE-Kennzeichen bestätigt.

Erläuterung: Klinische Prüfungen zur Konformitätsbewertung sind im MPG nur für Produkte der Klasse III (hohes Risiko) vorgeschrieben. Als →GCP für Medizinprodukte gelten die Normen EN-ISO 14155-1/2.

Mehrwertdienst

Definition: Technische Umsetzung von Anwendungen, die von der Telematik-Infrastruktur (TI) entweder nur Transportfunktionen oder auch Basisdienste nutzen und über die in § 291a SGB V definierten Anwendungsbereiche hinausgehen.

Meldung unerwünschter Ereignisse

→unerwünschtes Ereignis.

Monitor (Klinischer Monitor, Clinical Research Associate, CRA)

Definition: Der Klinische Monitor überwacht →Klinische Prüfungen, insbesondere nach →Arzneimittelgesetz.

Erläuterung: Das Monitoring umfasst die Kontrolle der Durchführung nach den Vorgaben der →Guten Klinischen Praxis (→Good Clinical Practice), der Deklaration von Helsinki und der entsprechenden Gesetze und Bestimmungen (u.a. →Arzneimittelgesetz, →Medizinprodukte-Gesetz) der einzelnen Länder, in denen die klinische Prüfung durchgeführt wird. Des Weiteren kontrolliert der

Monitor die Durchführung entsprechend der Vorgaben des →Prüfplans, die Dokumentation der entsprechenden Dokumentationsbögen und den Gebrauch der Studienmedikation.[47] Da Monitore im Rahmen der Überprüfung der Korrektheit der erfassten Daten auch Einblick in die Patientenakte als Quelldokumentation erhalten, sind Patienten im Rahmen der →Einwilligung über diesen Zugriff auf →personenbezogene Daten durch Dritte zu informieren.

Hinweis: In einem allgemeineren Sinn kann Monitor auch eine (meist) technische Überwachungseinrichtung bezeichnen.

MPG

siehe →Medizinprodukte-Gesetz

Multizentrische Studie

Definition: Eine Studie, die in mehreren Institutionen („Studienzentren") durchgeführt wird. →GCP-V § 3 (1): „Multizentrische klinische Prüfung ist eine nach einem einzigen →Prüfplan durchgeführte →klinische Prüfung, die in mehr als einer Prüfstelle erfolgt und daher von mehr als einem →Prüfer vorgenommen wird, wobei sich die weiteren Prüfstellen auch in anderen Mitgliedstaaten der Europäischen Union oder in Ländern befinden können, die nicht Mitgliedstaaten der Europäischen Union sind."

Erläuterung: Eine multizentrische Studie kann aus verschiedenen Gründen durchgeführt werden:

- An einzelnen Institutionen sind nicht genügend große Fallzahlen verfügbar.
- Der Einfluss von lokalen Faktoren (wie z.B. Anzahl und Qualifikation der behandelnden Ärzte oder verzerrte Auswahl von Probanden) auf das Studienergebnis soll bewertet oder gering gehalten werden.
- Eine weite Kooperation der Experten wird angestrebt.

Aus diesen Gründen sind die in medizinischen Forschungsverbünden durchgeführten Studien typischerweise multizentrisch.

Nichtinterventionelle Prüfung

siehe →nichtinterventionelle Studie.

Nichtinterventionelle Studie (nichtinterventionelle Prüfung)

Definition: Eine nichtinterventionelle Studie ist eine Untersuchung, in deren Rahmen Erkenntnisse aus der Behandlung von Personen mit Arzneimitteln gemäß den in der Zulassung festgelegten Angaben für deren Anwendung an-

47 vergl. http://de.wikipedia.org/wiki/Klinischer_Monitor (Abruf: 2014-08-27)

hand epidemiologischer Methoden analysiert werden; dabei folgt die Behandlung einschließlich der Diagnose und Überwachung nicht einem vorab festgelegten →Prüfplan, sondern ausschließlich der ärztlichen Praxis." [→AMG § 4 (3)]

Erläuterung: Es wird nur beobachtet, was während einer Behandlung nach ärztlicher Routine ohnehin passiert; die Behandlung wird nicht durch Festlegungen eines Studienprotokolls beeinflusst. Auch biomedizinische Forschung am Menschen oder epidemiologische Forschung mit →personenbezogenen Daten wird oft hier eingeordnet; diese Studientypen sind in der Regel nichtinterventionell. Siehe auch →Beobachtungsstudie.

Nutzer, Forscher, Kunde eines medizinischen Forschungsverbunds

Definition: Jeder, der die in einem →medizinischen Forschungsverbund vorhandene Daten oder Proben für ein →Forschungsvorhaben nutzt.

Erläuterung: Da Daten und Proben des medizinischen Forschungsverbunds für Forschungszwecke genutzt werden sollen, sind die Nutzer stets Forscher. Sie können der →Trägereinrichtung der Verbundes selbst angehören (= interne Forschung) oder aus anderen Einrichtungen kommen (= externe Forschung). Der Forscher als Nutzer tritt mit seinen Anforderungen (Spezifikation der Erkrankung, Randparameter wie Alter und Komorbiditäten, Anforderungen an die Daten oder Proben bzw. deren Analyse usw.) an den Forschungsverbund heran und erhält nach Durchlaufen eines geregelten Verfahrens Daten und gegebenenfalls auch Proben auf der Grundlage eines Abgabevertrags. Gehört der Forscher einer gewerblichen Einrichtung (etwa einem Pharma-Unternehmen) an und handelt auch der Forschungsverbund erwerbswirtschaftlich, hat der Forscher die Funktion eines Kunden.

Nutzungsordnung

siehe →Policy.

OrgDAT = Organisationsdaten

Definition: OrgDAT sind Begleitdaten eines Datensatzes oder einer Probe, die an unterschiedlichen Stellen erhoben werden können.

Erläuterung: Beispielsweise erfasst eine Proben gewinnende Stelle die Probenart und gegebenenfalls die Informationen zu Probenentnahme und Präanalytik. In der Probenbank werden die Begleitdaten einer Probe mit weiteren Informationen wie etwa den Umständen von Konservierung, Lagerung und Qualität gespeichert. Siehe auch →ADAT.

Patient

siehe →Proband.

Patientenaufklärung

siehe →Patienteninformation.

Patientenidentifikator

siehe →PID.

Patienteninformation (Aufklärung)

Definition: Mitteilung an den Teilnehmer eines →Forschungsvorhabens, was mit seinen Daten und ggf. →Proben passieren wird.

Erläuterung: Die Patienteninformation bildet die informationelle Grundlage für die nachfolgende →Einwilligungserklärung des Patienten oder Probanden in den Umgang des Forschungsverbundes mit den gewonnenen Daten und Proben („informed consent"). Die Patienteninformation enthält eine Fülle von Einzelangaben (Items), die dem Einwilligenden die Tragweite seiner nachfolgenden Einwilligungserklärung vor Augen führen soll. Für die Datenerhebung im Rahmen →klinischer Studien wurden Modelle solcher Patienteneinwilligungen entwickelt, die von der TMF auf die Besonderheiten bei →medizinischen Forschungsverbünden angepasst wurden.

Verweis: Vgl. zu den Einzelheiten [5].

Patientenliste (Identitätsmanagement für Patienten)

Definition: Zentrales Verzeichnis, das die Zuordnung von Patientenidentitäten (→IDAT) zu nichtsprechenden Identifikatoren (→PID) enthält.

Erläuterung: Da hier Identifikationsdaten verwaltet werden, besteht für die Patientenliste ein besonders hoher Anspruch auf Vertraulichkeit, d.h. insbesondere auf technischen Schutz.

Personenbezogenheit, Personenbeziehbarkeit

Definition: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)." [→BDSG § 3 (1)]

Erläuterung: Bei Daten bzw. Biomaterialien beziehen sich die Einzelangaben auf den Datensatz oder die Probe (Name des Probanden, Angaben zu dessen Gesundheitszustand usw.) oder ergeben sich aus der Probe bzw. deren Analyse, bei der etwa die genetische Ausstattung des Probanden ermittelt werden kann.

Man unterscheidet bei der Ausgestaltung des Personenbezugs eine grundsätzliche Personenbeziehbarkeit von der tatsächlichen Personenbezogenheit. Personenbeziehbarkeit setzt voraus, dass Angaben theoretisch einer Person zugeordnet werden können. Personenbezogenheit liegt dann vor, wenn diese

Zuordnung auch tatsächlich, ohne Aufwand vorgenommen werden kann, z.B. wenn die Person direkt und offen lesbar benannt wird. Das Gegenstück zur Personenbeziehbarkeit ist die Anonymität (s. →Anonymisierung). Eine Reduzierung der Personenbezogenheit erfolgt durch die →Pseudonymisierung.

Die befugte Wiederherstellung des Personenbezugs eines pseudonymisierten Datensatzes oder einer pseudonymisierten Probe erfolgt im Wege der →Depseudonymisierung.

Die unbefugte Wiederherstellung der Personenbezogenheit einer anonymisierten oder pseudonymisierten Probe wird als →Reidentifizierung bezeichnet. Um dies zu verhindern, ist das Rückidentifizierungsrisiko abzuschätzen, oft für jeden Einzelfall.

Hinweis: Zur Definition der Personenbezogenheit von Daten gibt es international unterschiedliche Auffassungen; das betrifft z.B. die Fragen: Sind pseudonyme Daten personenbeziehbar? Wie wird mit indirekter Personenbeziehbarkeit umgegangen?

Verweise: Zur allgemeinen Legaldefinition der Personenbezogenheit vgl. § 3 Abs. 1 BDSG; zu den Daten aus Proben und Analysen der Proben vgl. [2 S. 12ff].

PID = Patientenidentifikator

Definition: Der PID ist der eindeutige Ordnungsparameter für einen in einen Forschungsverbund eingeschlossenen →Patienten oder Probanden.

Erläuterung: Die Erzeugung des PID wird durch die anmeldende Stelle veranlasst. Der PID wird gemeinsam mit den →IDAT in der →Patientenliste gespeichert. In der Regel soll der PID nichtsprechend sein; er kann dann als →Pseudonym erster Stufe dienen.

Policy (Richtlinie, Leitlinie, Sicherheitspolicy, Regelwerke, Nutzungsordnung)

Definition: Policies und Nutzungsordnungen stellen Regelwerke für zentrale Dienste bereit, die das Sicherheitspotenzial der eingesetzten technischen Instrumente sowie den Zugriff und die Verwendung geschützter Daten festlegen und organisatorisch in definierten Verantwortlichkeiten verankern. Die Betreiber und die Nutzer werden über die notwendigen Maßnahmen und Abläufe informiert und zu einem planmäßigen, regelgerechten Handeln verpflichtet.

Erläuterung: Richtlinien sind meist von Institutionen veröffentlichte Regeln des Handelns und Unterlassens, die dem einzelnen Anwender einen geringen Ermessensspielraum einräumen. Ihre Nichtbeachtung kann Sanktionen nach sich ziehen. Eine ähnliche Verbindlichkeit wie Richtlinien haben Standards, die als normative Vorgaben bezüglich der Erfüllung von Qualitätsanforderungen verstanden werden und durch ihre in der Regel exakte Beschreibung einen mehr technisch-imperativen Charakter haben. Demgegenüber sind Leitlinien

systematisch entwickelte Entscheidungshilfen über angemessene Vorgehensweisen bei speziellen (in der Medizin: diagnostischen und therapeutischen) Problemstellungen, von denen in begründeten Einzelfällen auch abgewichen werden kann. Sie lassen dem Anwender also einen Entscheidungsspielraum.

Für alle klinikübergreifenden Dienste in einem →Forschungsverbund sind die Auftragsbedingungen und Nutzungsordnungen festzulegen, welche die Maßnahmen zum Datenschutz konkretisieren.

Hinweis: Der englische Begriff Policy bezeichnet die inhaltliche Dimension von Politik.

Principal Investigator (Studienleiter)

Definition: Der Forscher, der die wissenschaftliche Hauptverantwortung für die →Studie trägt. „Wird eine Prüfung in mehreren Prüfstellen durchgeführt, wird vom →Sponsor ein →Prüfer als Leiter der →klinischen Prüfung benannt." [→AMG § 4]

Erläuterung: Bei →Arzneimittelstudien ist der Studienleiter meistens kein Angestellter des Sponsors. Bei →Therapieoptimierungsstudien, die nicht dem AMG unterliegen, nimmt der Studienleiter oft im Sinne eines →Konsils Einfluss auf die Behandlung.

Proband, Patient

Definition: Patient und Proband sind die Personen, die dem →Forschungsverbund Daten zu ihrer Gesundheit und Materialien ihres Körpers zu Zwecken der biomedizinischen Forschung zur Verfügung stellen. Erfolgt die Datengewinnung oder Probenentnahme im →Behandlungszusammenhang, ist der Spender „Patient". Erfolgt die Datengewinnung oder Probenentnahme im →Forschungszusammenhang, ist der Spender „Proband". Der Begriff „Proband" wird auch als Oberbegriff für „Patient und/oder Proband" verwendet, insbesondere, wenn eine →Kontrollgruppe in die Studie involviert ist.

Erläuterung: Vom Patienten bzw. Probanden ist die →Einwilligungserklärung einzuholen, die über die Weiterverwendung der Daten und Proben zu Forschungszwecken entscheidet. Mit ihm ist ggf. auch ein Vertrag abzuschließen, in dem die Eigentums- und Nutzungsrechte an Proben festgelegt werden.

Verweise: Siehe dazu auch die Begriffe →Einwilligungserklärung, →Patienteninformation und →Widerruf.

Probandenvertrag

Definition: Ein zwischen Arzt und →Proband im Rahmen →klinischer Studien zustande kommender zivilrechtlicher Vertrag. Häufig wird das Grundmuster

eines Dienstleistungsvertrags zugrunde gelegt, demnach ist der →Patient der Dienstleister und der Arzt der Dienstleistungsempfänger.

Erläuterung: Der Probandenvertrag muss nicht explizit abgeschlossen werden, er kann auch implizit durch schlüssiges Verhalten beider Seiten zustande kommen. Im Vergleich zu einem Behandlungsvertrag, bei dem der Arzt der Dienstleister und der →Patient der Dienstleistungsempfänger ist, findet ein Rollentausch der Vertragspartner statt.

ProbDAT = Probenanalysedaten

Definition: Die mit ProbDAT bezeichneten Ergebnisse der Probenanalyse werden je nach Bedarf an anfragende Forscher übermittelt.

Erläuterung: Die ihnen zu Grunde liegenden Analysen können sowohl von den der Probenbank angeschlossenen Labors als auch von kooperierenden Einrichtungen durchgeführt werden. ProbDAT können potenziell rückbeziehbare Daten darstellen, wie etwa im Fall von Genotypen. Ihre Speicherung sollte daher separat von anderen Daten erfolgen.

Probe (Material, Biomaterial)

Definition: Dem menschlichen Körper zu diagnostischen oder wissenschaftlichen Zwecken entnommene Substanz.

Erläuterung: Der Begriff Probe wird im Zusammenhang mit →Biobanken synonym zum Begriff Material oder Biomaterial verwendet. Beispiele für Proben unterschiedlichster Art sind etwa:

- Gewebe,
- Körperflüssigkeiten,
- Zellen,
- RNA,
- DNA,
- Organe.

Probenanalysedaten

siehe →ProbDAT.

Probenbank

siehe →Biobank.

Probennummer

siehe →LabID.

Probensammlung

siehe →Biobank.

Prüfarzt (Prüfer)

Definition: „Prüfer ist in der Regel ein für die Durchführung der →klinischen Prüfung bei Menschen in einer Prüfstelle verantwortlicher Arzt oder in begründeten Ausnahmefällen eine andere Person, deren Beruf auf Grund seiner wissenschaftlichen Anforderungen und der seine Ausübung voraussetzenden Erfahrungen in der Patientenbetreuung für die Durchführung von Forschungen am Menschen qualifiziert." [→AMG § 4]

Erläuterung: Der Prüfarzt in einer klinischen Studie ist derjenige, der direkten Kontakt zum Patienten hat. Mit ihm besteht ein →Behandlungszusammenhang.

Prüfer

siehe →Prüfarzt.

Prüfplan

Definition: →GCP-V § 3 (2): „Prüfplan ist die Beschreibung der Zielsetzung, Planung, Methodik, statistischen Erwägungen und Organisation einer →klinischen Prüfung."

Pseudonym

siehe →PSN.

Pseudonymisierung (Codierung)

Definition: „Die Pseudonymisierung ist das Ersetzen des Namens oder anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." [→BDSG § 3 (6a)].

Erläuterung: Dies kann beispielsweise durch die Ersetzung des Probanden-Namens durch eine Kenn-Nummer geschehen. Man kann die Pseudonymisierung daher als eine eingeschränkte →Anonymisierung auffassen. Ziel der Pseudonymisierung ist es aber nicht, den Personenbezug irreversibel abzutrennen, sondern lediglich durch ein eindeutiges Kennzeichen – ein Pseudonym – zu ersetzen, das für sich genommen die Identifikation der dahinterstehenden Person ausschließt oder aber wesentlich erschwert.

Grundsätzlich bleiben pseudonymisierte Daten allerdings →personenbeziehbar: Es existiert ein „Geheimnisträger", der die Zuordnung von Person zu Pseu-

donym kennt oder wiederherstellen kann und entsprechend vertrauenswürdig und geschützt sein muss.

Der Nutzen, diese Abschwächung der Reduktion des Personenbezugs in Kauf zu nehmen, besteht in der Möglichkeit, die individuelle Veränderung personenbezogener Daten, z.B. einen Krankheitsverlauf, über die Zeit zu studieren, wofür eine mehrfache Zuordnung von Daten zur identischen Person zu verschiedenen Zeitpunkten erforderlich ist, ohne dass während dieses langen Beobachtungszeitraum die Identität der Person bekannt sein muss.

Man unterscheidet unterschiedliche Verfahren zur Pseudonymisierung (einstufige und mehrstufige Pseudonymisierung, Einweg-Verfahren zur Pseudonymisierung, dezentrale und zentrale Pseudonymisierung u.a.).

Achtung: Das oft verwendete Verfahren, die Identitätsdaten durch ein Kürzel aus Initialen und Geburtsdatum zu ersetzen, ist als Pseudonymisierung nicht geeignet.

Hinweis: Die Pseudonymisierung wird bezüglich der Sicherheit gegen Wiederherstellung der →Personenbezogenheit durch die →Anonymisierung übertroffen.

Verweise: Zur Legaldefinition der Pseudonymisierung vgl. § 3 Abs. 6a BDSG, siehe auch die Begriffe →Anonymisierung, →Personenbezogenheit, →Depseudonymisierung, →Reidentifizierung.

PSN = Pseudonym

Definition: Das PSN ist ein nichtsprechender Identifikator eines Patienten oder Probanden (Buchstaben oder Zahlen, die nicht auf die personenidentifizierenden Daten rückschließen lassen).

Erläuterung: Im Konzept der TMF wird das PSN durch kryptographische Verschlüsselung des →PID erzeugt. Die TMF stellt dafür eine Netzkomponente „Pseudonymisierungsdienst“ zur Verfügung.

Public Use File

Definition: Öffentlich zugängliche Datensammlung, die im Regelfall aufgrund unvorhersehbaren Zusatzwissens der Nutzer absolut →anonymisiert sein muss.

Erläuterung: Für die →Anonymisierung solcher Datensammlungen wird das Verfahren der →k-Anonymisierung empfohlen. Abzugrenzen von Public-Use-Files sind →Scientific-Use-Files.

Qualitätssicherung

siehe →Datenqualität

Querschnittstudie

Definition: Eine Querschnittstudie ermittelt eine Momentaufnahme der untersuchten epidemiologischen Daten in einer Population.

Erläuterung: Durch den zeitlichen „Schnappschuss“ der epidemiologischen Daten sind die aus der Studie gezogenen kausalen Zusammenhänge zwischen Exposition und Erkrankung schwach und dienen mehr der Generierung von Hypothesen als deren Verifizierung.

RDE

→Remote Data Entry

Recht auf Nichtwissen

Definition: Besonders im Zusammenhang genetischer Analyseergebnisse postuliertes Recht des Betroffenen, diese nicht zur Kenntnis nehmen zu müssen.

Erläuterung: Dieses Recht auf Nichtwissen und damit auf Unkenntnis des persönlichen Schicksals ergibt sich aus den Grundrechten des Menschen, insbesondere dem Recht auf freie Entfaltung der Persönlichkeit (§ 1 und 2 GG). Gleichzeitig impliziert dieses Recht auch die Rechte auf Kenntnis persönlicher Daten und auf eine Selbstbestimmung bei der Information. Zu diesem Schluss kommt die Enquete-Kommission „Recht und Ethik der modernen Medizin“ in ihrem Schlussbericht: „Eingriffe in das Recht auf Nichtwissen bedürfen einer Rechtfertigung. Dieses Recht schützt die Einzelne bzw. den Einzelnen vor Informationen über ihre bzw. seine gesundheitliche Situation, die sie bzw. er nicht zu erlangen bzw. zu besitzen wünscht.“ [24 S. 132].

Regelwerk

siehe →Policy.

Register

Definition: Ein Register ist eine systematische Sammlung von Informationen zu bestimmten Erkrankungen. Charakteristikum eines Registers ist die angestrebte Vollzähligkeit (typischerweise mindestens 95% aller einschlägigen Fälle).

Erläuterung: Besonders verbreitet sind Krebsregister. Man unterscheidet epidemiologische Register und klinische Register.

Mit epidemiologischen Registern wird das Krankheitsgeschehen, z.B. die Häufigkeit von Erkrankungen in einer Region oder einer Zeitspanne, beobachtet.

Klinische Register zielen darauf, die Behandlung zu verbessern. Dazu müssen zunächst relativ detailliert Daten zur Erkrankung und zur Therapie gesammelt

werden. Neben der kontinuierlichen Auswertung wird auch die Optimierung der individuellen Betreuung angestrebt. Über Erinnerungsverfahren wird sichergestellt, dass Therapien und Nachsorgeuntersuchungen zu festgelegten Zeitpunkten stattfinden. Ferner soll erreicht werden, dass jeder an der Betreuung Beteiligte die nötigen Informationen zur Verfügung hat. Ein Register kann somit im →Versorgungs- oder →Forschungszusammenhang stehen.

In manchen Situationen, z.B. bei seltenen Erkrankungen, ist sinnvolle epidemiologische, ja oft sogar klinische Forschung erst durch Datensammlung in Registern möglich.

Verweise: →klinische Datenbank, →ForschungsdatenbankH_Klinische_Datenbank

Reidentifizierung

Definition: Im Wege der Reidentifizierung wird der →Personenbezug von →anonymisierten oder →pseudonymisierten →Daten und →Proben unbefugt wiederhergestellt.

Erläuterung: Eine Reidentifizierung kann einerseits durch Korrumpierung eines Pseudonyms oder eines Anonymisierungs- oder Pseudonymisierungsverfahrens erfolgen. Andererseits kann eine hinreichende Konstellation von in der Summe eindeutig einer Person zuzuweisenden Daten („Alleinstellungsmerkmalen“) im formal anonymisierten Datensatz vorliegen. Ist diese Datenkonstellation in Vergleichsdatenbanken oder in persönlichem Wissen mit offenem Personenbezug bekannt, so kann aus dem Inhalt der Daten – trotz formaler Abtrennung der personenidentfzierenden Daten – auf die Person rückgeschlossen werden, d.h. es kann eine Reidentifizierung durch Inferenzen auf der Basis datenimmanenter Identifizierungsrisiken erfolgen.

Von der Reidentifizierung ist die →Depseudonymisierung zu unterscheiden, die durch Umkehrung des Pseudonymisierungsverfahrens den Personenbezug befugt rekonstruiert.

Verwandte Begriffe: →Anonymisierung und →Pseudonymisierung.

Remote Data Entry (RDE)/Electronic Data Capture (EDC)

Definition: Verfahren zur zentralen Erfassung von Studiendaten bei dezentraler Dateneingabe auf Basis von Software-Systemen, die eine im Regelfall webbasierte Präsentation von →Dokumentationsbögen (CRFs) ermöglichen.

Richtlinie

siehe →Policy

Rückidentifizierung (Reidentifikation)

siehe →Reidentifizierung

SAE

siehe →unerwünschtes Ereignis.

Schweigepflicht

Definition: Die ärztliche Schweigepflicht ist die ethische und rechtliche Pflicht des Arztes, Verschwiegenheit über alles zu wahren, was ihm bei der Ausübung seines Berufes über einen Patienten bekannt wird (Wahrung des Patientengeheimnisses).

Erläuterung: Schon die Tatsache des Arztbesuchs fällt unter die Schweigepflicht. Die Schweigepflicht gilt für den Arzt, Zahnarzt, den Angehörigen eines anderen Heilberufs, der eine staatlich geregelte Ausbildung erfordert, für Angehörige medizinisch-technischer Assistenzberufe, medizinische Dokumentare und für medizinische Informatiker, sofern sie zum Behandlungsteam des verantwortlichen Arztes gehören, d.h. seiner direkten Weisungsbefugnis unterliegen.

Verweise: Rechtsgrundlage in §§ 203, 204 StGB in Verbindung mit § 3 Musterberufsordnung; in den Vorschriften des Strafgesetzbuches wird die Verletzung der Schweigepflicht unter Strafe gestellt; siehe auch den Eintrag „Schweigepflicht“ in [48]. Ferner die Empfehlungen der Bundesärztekammer zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis [49].

Scientific Use Files

Definition: Für bestimmte Forschungsfragestellungen und nach einem formal festgelegten Prüfungsverfahren zugängliche Datensammlungen, die →anonymisiert oder bei Vorliegen einer entsprechenden →Einwilligung auch →pseudonymisiert sein können.

SDB

siehe →Studiendatenbank

Selbstbestimmungsrecht, informationelles

Definition: Das informationelle Selbstbestimmungsrecht ist das Recht jedes Menschen, grundsätzlich selbst darüber zu bestimmen, wer was wann und bei welcher Gelegenheit über ihn erfährt.

Erläuterung: Das informationelle Selbstbestimmungsrecht basiert nach der grundsätzlichen Entscheidung des Bundesverfassungsgerichts im „Volkszählungsurteil" aus dem Jahr 1983 auf den Grundrechten des Art. 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit) sowie des Art. 1 Abs. 1 GG (Schutz der Menschenwürde). Freie Entfaltung der Persönlichkeit setzt nach dieser Entscheidung des Bundesverfassungsgerichts unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Ihren gesetzlichen Niederschlag finden diese Grundaussagen des Bundesverfassungsgerichts in den Vorschriften der Datenschutzgesetze sowie in datenschutzrelevanten Vorschriften vieler anderer Gesetze.

Verweise: Das „Volkszählungsurteil" des Bundesverfassungsgerichts aus dem Jahr 1983 [50 S. 42f.], Bundesdatenschutzgesetz online unter http://www.gesetze-im-internet.de/bdsg_1990/

Seltene Erkrankung

Definition: In Europa bezeichnet man eine Erkrankung als selten, wenn sie weniger als einen unter 2.000 Menschen im Laufe seines Lebens trifft. Das bedeutet, dass in Deutschland auch über längere Zeiträume hinweg oft nur wenige hundert Fälle auftreten. Von den ungefähr 30.000 bekannten Krankheiten werden 5.000 bis 7.000 zu den seltenen Erkrankungen gerechnet.

Verweis: [7]

SIC (Subject Identification Code)

Der SIC (Subject Identification Code) ist das in →AMG und →GCP vorgesehene Pseudonym, das als Ordnungsmerkmal in der →SDB und zum Export an den →Sponsor dient. Er ist (im Gegensatz zum →PID) dem →Prüfarzt bekannt.

SOP

siehe →Standard Operating Procedure

Sponsor

Definition: Auftraggeber und Hauptverantwortlicher einer →Studie. Bei Arzneimittelstudien ist der Sponsor in der Regel ein Pharma-Unternehmen, bei wissenschaftsgetriebenen Studien (→IIT) in der Regel die Universität oder Forschungseinrichtung, der der Initiator der Studie angehört. „Sponsor ist eine natürliche

oder juristische Person, die die Verantwortung für die Veranlassung, Organisation und Finanzierung einer klinischen Prüfung bei Menschen übernimmt." [→AMG § 4]

Erläuterung: Als Sponsoren klinischer Studien treten die pharmazeutische Industrie, Universitätsinstitute oder -kliniken sowie staatliche, halbstaatliche und sonstige Forschungsinstitute und Einrichtungen des Gesundheitswesens auf.

Stammdaten

siehe →IDAT.

Standard Operating Procedure (SOP, Standardarbeitsanweisung)

Definition: Dokument, welches das Vorgehen innerhalb eines Arbeitsprozesses beschreibt.

Erläuterung: Häufig wiederkehrende Arbeitsabläufe werden beschrieben und den Ausführenden erklärend an die Hand gegeben.

Studie

siehe →Forschungsvorhaben.

Studiendatenbank (SDB)

Definition: Datenbank, in der die Daten einer oder mehrerer, auch →multizentrischer, →klinischer oder →epidemiologischer Studien zentral gesammelt und verwaltet werden.

Erläuterung: Studiendatenbanken enthalten in Abgrenzung zu →Klinischen Datenbanken explizit im Forschungskontext (→Forschungszusammenhang) erhobene Daten.

Studienleiter

siehe →Principal Investigator.

Studienzentrale

Definition: Durch die →Studienleitung für die Datenerfassung, →Qualitätssicherung und Datenverarbeitung beauftragte Einrichtung.

SUE

siehe →unerwünschtes Ereignis.

SUSAR

siehe →unerwünschtes Ereignis.

Therapieoptimierungsstudie

Definition: Klinische Studie, bei der verschiedene Optionen eines Therapieverfahrens miteinander verglichen werden. Die Patienten werden verschiedenen Studienarmen zugeteilt.

Erläuterung: Therapieoptimierungsstudien sind vor allem bei komplexen Therapieformen im Rahmen der Krebsbehandlung verbreitet.

Ticket (Zugriffsticket/Token)

Definition: Nur für eine Transaktion gültige Zufallskennung (zufällige, längere Folge alphanumerischer Zeichen).

Erläuterung: Zugriffstickets werden im Zusammenhang mit einer →Klinischen Datenbank für die sichere Zusammenführung von →IDAT und →MDAT ohne Offenbarung des →PID verwendet. Im früheren Modell A der generischen Datenschutzkonzepte der TMF [1] wurde hierfür der Begriff TempID eingeführt.

Träger des medizinischen Forschungsverbundes

Definition: Träger des →medizinischen Forschungsverbundes ist die Einrichtung oder Institution, die rechtlich für die Daten- und Probensammlung verantwortlich ist.

Erläuterung: Dies kann eine Universität, eine Klinik oder ein Zusammenschluss verschiedenartiger Einrichtungen in Form einer juristischen Person (etwa einer GmbH oder eines eingetragenen Vereins) oder einer anderen Rechtsform (Gesellschaft bürgerlichen Rechts, Stiftung des privaten Rechts usw.) sein. Der Träger des medizinischen Forschungsverbundes kann den eigentlichen Datenbank- oder Biomaterialbank-Betrieb einer anderen Stelle (dem sogenannten Betreiber) übertragen. Dieser Betreiber muss nicht notwendigerweise der Träger-Institution der Biobank angehören. Hierbei handelt es sich dann um eine Datenverarbeitung im Auftrag.

Verweis: Zur Frage der rechtlichen Ausgestaltung des Trägers einer Biobank siehe [23]

Treuhänder

→Datentreuhänder

Unerwünschtes Ereignis

Definition: Ein unerwünschtes Ereignis ist ein Nebeneffekt einer medizinischen Therapie, der für den Patienten unangenehm oder schädlich ist.

Erläuterung: Ein solcher Nebeneffekt kann bei regelgerechter Therapiedurchführung auftreten, aber auch das Ergebnis einer falschen oder ungeeigneten Dosierung eines Medikaments oder einer nicht sachgemäß durchgeführten sonstigen therapeutischen Maßnahme sein. Er kann auch als Wechselwirkung zwischen verschiedenen Medikamenten auftreten. Unterschieden werden

- Unerwünschtes Ereignis (Adverse Effect, AE): „jedes nachteilige Vorkommen, das einer betroffenen Person widerfährt, der ein Prüfpräparat verabreicht wurde, und das nicht notwendigerweise in ursächlichem Zusammenhang mit dieser Behandlung steht" [→GCP-V § 3 (6)];
- Nebenwirkung (Adverse Reaction, AR): „jede nachteilige und unbeabsichtigte Reaktion auf ein Prüfpräparat unabhängig von dessen Dosierung" [→GCP-V § 3 (7)];
- Unerwartete Nebenwirkung (Unexpected Adverse Reaction, UAR): „Nebenwirkung, die nach Art oder Schweregrad nicht mit der vorliegenden Information über das Prüfpräparat übereinstimmt" [→GCP-V § 3 (9)];
- Schwerwiegendes unerwünschtes Ereignis oder schwerwiegende Nebenwirkung (Serious Adverse Event, SAE; Serious Adverse Reaction, SAR): ein AE oder eine AR, die „unabhängig von der Dosis tödlich oder lebensbedrohend ist, eine stationäre Behandlung oder deren Verlängerung erforderlich macht, zu einer bleibenden oder schwerwiegenden Behinderung oder Invalidität führt oder eine kongenitale Anomalie oder einen Geburtsfehler zur Folge hat" [→GCP-V § 3 (8)];
- Schweres unerwünschtes Ereignis (Serious Unwanted Event, SUE) sowie
- Verdachtsfall unerwarteter schwerwiegender Nebenwirkung (Suspected Unexpected Serious Adverse Reaction, SUSAR).

Für →klinische Prüfungen definieren das →AMG im § 63b und die →GCP-V in §§ 12–13 Meldepflichten und -verfahren.

Validierung

Definition: Erbringen eines dokumentierten Nachweises, dass ein System oder Prozess in Übereinstimmung mit seinen Anforderungen funktioniert.

Erläuterung: In den GxP-Richtlinien (Good x Practice, x = Laboratory, Clinical oder Manufacturing, GLP, →GCP, GMP) wird gefordert, dass pharmazeutische Unternehmen ihre Prozesse mit Einfluss auf die Produktqualität validieren und die zugehörigen Geräte qualifizieren müssen. Diese regulatorischen Anforderungen gelten auch für computergestützte Systeme, die aus Hard- und Software bestehen.

Verhältnismäßigkeit

Definition: Datenschutzmaßnahmen sollen in einem angemessenen Verhältnis zum Schutzzweck stehen. Die Verhältnismäßigkeit bezieht sich dabei auf die Relation des Aufwands zum Nutzen bzw. zum verhinderten Schaden.

Erläuterung: Verhältnismäßigkeit bedeutet in der Regel nicht, dass ein kontinuierlicher Sicherheitsparameter mehr oder weniger hoch angesetzt wird, sondern dass Redundanzen vermehrt oder abgebaut werden. So können bei hohem Schutzbedarf der Daten technische Zugangsbarrieren mit organisatorischen Regelungen verknüpft werden, wohingegen bei geringerem Schutzbedarf vielleicht die technischen Maßnahmen alleine ausreichen.

Versorgungsdatenbank

siehe →Klinische Datenbank

Widerruf

Definition: Unter dem Widerruf der Daten- oder Probenverwendung versteht man die teilweise oder vollständige Rücknahme der →Einwilligungserklärung (s. dort) mit der Folge, dass Daten (→Datenkategorien) und →Proben vom →Forschungsverbund nicht bzw. nur noch in eingeschränktem Maße für eigene oder fremde →Forschungsvorhaben verwendet werden dürfen. Aus der Vereinbarung mit dem →Patienten oder Probanden kann sich nach dem Widerruf der →Einwilligungserklärung auch die Pflicht ergeben, Daten zu löschen oder zu →anonymisieren bzw. die →Probe an den Probanden herauszugeben, sie zu vernichten oder zumindest zu →anonymisieren. Es sind auch Fälle denkbar, in denen ein Widerruf der →Einwilligungserklärung ausgeschlossen ist (etwa nach dem →AMG).

Erläuterung: Zieht ein Patient seine Teilnahme am Forschungsverbund zurück oder verstirbt ein im Forschungsverbund erfasster Patient, so sind in jedem Fall die Identifikationsdaten (→IDAT) des Patienten in allen Dateien bzw. Registern außerhalb der lokalen Dokumentation der behandelnden Einrichtung zu löschen. Medizinische Daten (→MDAT) müssen – je nach Verfügung in der Einwilligung – gelöscht oder anonymisiert werden.

Verweise: Weitere Hinweise finden sich beim Begriff der →Einwilligungserklärung und in dem generischen Datenschutzkonzept der TMF für Biobanken [2 S. 42ff.].

Wissenschaftsgetriebene Studie

siehe →Investigator Initiated Trial

Abkürzungsverzeichnis

AAL	Ambient Assisted Living
ACL	Access Control List
AE	Adverse Event, unerwünschtes Ereignis im Rahmen einer Arzneitmittelprüfung
AES	Advanced Encryption Standard: symmetrisches Verschlüsselungsverfahren
AG	Aktiengesellschaft
AG	Arbeitsgruppe
AK	Arbeitskreis
AK EK	Arbeitskreis Medizinischer Ethik-Kommissionen in der Bundesrepublik Deutschland (www.ak-med-ethik-komm.de)
AMG	Gesetz über den Verkehr mit Arzneimitteln – Arzneimittelgesetz
AMIA	American Medical Informatics Association (www.amia.org)
AR	Adverse Reaction, Nebenwirkung im Rahmen einer Arzneimittelprüfung
BayDSG	Bayerisches Datenschutzgesetz
BayKrG	Bayerisches Krankenhausgesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMB	Biomaterialbank(en)
BMBF	Bundesministerium für Bildung und Forschung (www.bmbf.de)
BMWi	Bundesministerium für Wirtschaft und Technologie (www.bmwi.bund.de)
BSG	Bundessozialgericht (www.bundessozialgericht.de)
BSI	Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de)
CA	Certification Authority, im Rahmen einer PKI für die Überprüfung öffentlicher Schlüssel und Herausgabe zugehöriger Zertifikate verantwortlich
CDISC	Clinical Data Interchange Standards Consortium (www.cdisc.org)
CDM	Clinical Data Manager
CE	Conformité Européenne (franz.): Kennzeichnung der Produktsicherheit nach EU-Recht
CEN	Comité Européen de Normalisation, Europäisches Komitee für Normung (www.cenorm.be)
CGI	Common Gateway Interface: Standardschnittstelle zur Kommunikation zwischen Webclient und Webserver
CIO	Chief Information Officer
cloud4health	im Rahmen des BMWi-Förderprogramms „Trusted Cloud" gefördertes Projekt zur Entwicklung und Erprobung von innovativen, sicheren und rechtskonformen Cloud-Computing-Diensten im Gesundheitsbereich (www.cloud4health.de)
CRA	Clinical Research Associate

CRF	Case Report Form
CRM	Customer Relationship Management
CRO	Contract Research Organisation
CT	Computer-Tomografie
DB	Datenbank
DES	Data Encryption Standard; symmetrischer Verschlüsselungsalgorithmus
DFG	Deutsche Forschungsgemeinschaft (www.dfg.de)
DGEpi	Deutsche Gesellschaft für Epidemiologie e.V. (http://dgepi.de)
D-Grid	Vom BMBF gefördertes Integrationsprojekt für den Aufbau und die Nutzung von GRID-Infrastrukturen in verschiedenen Anwendungsbereichen (www.d-grid.de)
DGSMP	Deutsche Gesellschaft für Sozialmedizin und Prävention e.V. (www.dgsmp.de)
DGVO	Datenschutzgrundverordnung
DICOM	Digital Imaging and Communications in Medicine (http://medical.nema.org)
DKKR	Deutsches Kinderkrebsregister (www.kinderkrebsregister.de)
DNA	Deoxyribonucleic acid (Desoxyribonukleinsäure)
DSG	Datenschutzgesetz
DuD	Zeitschrift „Datenschutz und Datensicherheit“ (www.dud.de)
E2B	ICH-Code der Richtlinie „Data Elements for Transmission of Individual Case Safety Reports“
EB	Epidermolysis Bullosa
eCRF	electronic Case Report Form
EDC	Electronic Data Capturing
EFA	Elektronische Fallakte
EG	Europäische Gemeinschaft
eGA	Elektronische Gesundheitsakte
EGA	siehe eGA
eGK	elektronische Gesundheitskarte (www.die-gesundheitskarte.de)
EMA	European Medicines Agency (www.ema.europa.eu)
EMEA	siehe EMA
EN	Europäische Norm des CEN
EPA	Elektronische Patientenakte
ETL	Extract, Transform, Load: Kurzform für den Prozess, Daten aus mehreren, heterogenen Datenquellen selektiv zu lesen, zu transformieren und in einer einheitlichen Zielstruktur abzuspeichern
EuGH	Gerichtshof der Europäischen Gemeinschaften (http://curia.europa.eu)
EWG	Europäische Wirtschaftsgemeinschaft

FDB	Forschungsdatenbank
FK	Fall-Kontroll(-Studie)
GCP	Good Clinical Practice, Regelwerk der ICH
GCP-V	Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen – GCP-Verordnung
GEP	Gute Epidemiologische Praxis
GG	Grundgesetz der Bundesrepublik Deutschland
GKV	Gesetzliche Krankenversicherung
GLP	Good Laboratory Practice
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (www.gmds.de)
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung – GKV-Modernisierungsgesetz
GMP	Good Manufacturing Practice, Richtlinien der Weltgesundheitsorganisation (WHO) für die Herstellung und die Sicherung der Qualität von Arzneimitteln
GPS	Gute Praxis Sekundäratenanalyse der DGSMP, DGEpi, GMDS und DGSMP
GRID	Computernetz für verteiltes Rechnen und Anwendungen, die verteiltes Rechnen voraussetzen
GxP	Good x Practice, x = Laboratory, Clinical oder Manufacturing
HBA	Heilberufeausweis
HDSG	Hessisches Datenschutzgesetz
HIV	Human Immunodeficiency Virus
HL7	Health Level Seven; Internationale SDO für den Bereich der Interoperabilität von IT-Systemen im Gesundheitswesen (www.hl7.org)
Homonym	Zusammenführung von Datensätzen zu unterschiedlichen Personen in einem Datensatz mit einem PID
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
I2B2	Informatics for Integrating Biology and the Bedside (www.i2b2.org)
IaaS	Infrastructure as a Service
ICH	International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (www.ich.org)
ID	Identifikationsnummer
IDAT	Identifizierende Daten (eines Patienten)
IHE	Integrating the Healthcare Enterprise (www.ihe.net)
IIT	Investigator initiated trial
ISO 27001	ISO-Standard zum IT-Sicherheitsmanagement: „Information Technology – Security Techniques – Information Security Management Systems – Requirements“

ISO	International Organization for Standardization (www.iso.org)
IZKS	Interdisziplinäres Zentrum Klinische Studien
JPEG	Komprimiertes Bilddateiformat der Joint Photographic Experts Group (www.jpeg.org)
KA	Registerzeichen beim BSG für Vertrags(zahn)arztrecht
k-Anonymität	Eine Datensammlung ist k-anonym, wenn jede Merkmalskombination, die potenziell für einen reidentifizierenden Abgleich genutzt werden könnte, in mindestens k Datensätzen vorkommt
KDB	Klinische Datenbank
KKS	Koordinierungszentrum für Klinische Studien (www.kks-netzwerk.de)
KN	Kompetenznetz (www.kompetenznetze-medizin.de)
KPOH	KN Pädiatrische Onkologie und Hämatologie (www.kompetenznetz-paed-onkologie.de)
LabID	Labordaten-/Probennummer
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragte(r) für den Datenschutz
LKG	Landeskrankenhausgesetz(e)
MBO	Musterberufsordnung für Ärzte
MDAT	Medizinische Daten
MPG	Gesetz über Medizinprodukte – Medizinproduktegesetz
MPKPV	Verordnung über klinische Prüfungen von Medizinprodukten
MRT	Magnetresonanztomographie
NIH	US National Institutes of Health (www.nih.gov)
NRW	Nordrhein-Westfalen
OASIS	Organization for the Advancement of Structured Information Standards (www.oasis-open.org)
OP	Operation, Operationssaal
PaaS	Platform as a Service
Patientenfach	Elektronischer Datencontainer auf der eGK oder in der zugehörigen Telematikinfrastruktur für die Ablage und Übermittlung von vom Versicherten selbst oder für diesen zur Verfügung gestellten Daten, die sich ausschließlich in der Datenhoheit des Versicherten befinden
PDF	Portable Document Format von Adobe (www.adobe.com)
PET	Positronenemissionstomographie
PID	Patientenidentifikator
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PL	Patientenliste

PneumoGrid Vom BMBF gefördertes Projekt zur Entwicklung einer gridbasierten Infrastruktur und darauf aufbauender Dienste zur Unterstützung von Diagnostik und Therapie der chronisch obstruktiven Lungenerkrankung (www.pneumogrid.de)

PSD Pseudonymisierungsdienst (der TMF)

PSN Pseudonym

PStG Personenstandsgesetz

QS Qualitätssicherung

RDE Remote Data Entry (System)

RFD Retrieve Form for Data Capture; IHE IT Infrastructure Technical Framework

RN Randnummer

RNA Ribonukleinsäure

RöV Verordnung über den Schutz vor Schäden durch Röntgenstrahlen – Röntgenverordnung

SaaS Software as a Service

SAE Serious Adverse Event, schwerwiegendes unerwünschtes Ereignis im Rahmen einer Arzneimittelprüfung

SAML Security Assertion Markup Language, XML-basierte Auszeichnungssprache zur Beschreibung von sicherheitsbezogenen Informationen

SAR Serious Adverse Reaction, schwerwiegende Nebenwirkung im Rahmen einer Arzneimittelprüfung

SCORM Sharable Content Object Reference Model (www.adlnet.gov/scorm/index.cfm)

SDB Studiendatenbank

SDO Standards Development Organization

SGB Sozialgesetzbuch

SIC Subject Identification Code

SLA Service Level Agreement

SN Sequencing and Navigation; Teilspezifikation von SCORM

SOAP Simple Object Access Protocol; vom W3C empfohlener, XML-basierter Protokoll-Standard zur Kommunikation strukturierter Daten mit Webservices per HTTP

SOP Standard Operating Procedure

SQL Structured Query Language (Standard-Sprache für Datenbank-Zugriff)

SSL Secure Socket Layer, verschlüsselte HTTP-Verbindung

StGB Strafgesetzbuch

StPO Strafprozessordnung

StrlSchV Verordnung über den Schutz vor Schäden durch ionisierende Strahlen – Strahlenschutzverordnung

SUE Serious Unexpected Event

SUSAR	Suspected Serious Unexpected Adverse Reaction; Verdachtsfall einer unerwarteten schwerwiegenden Nebenwirkung im Rahmen einer Arzneimittelprüfung
Synonym	Anlage mehrerer Datensätze zu einer Person mit jeweils unterschiedlichem PID
TKT	Ticket, auch Zugriffsticket
TLS	Transport Layer Security
TMF	TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (www.tmf-ev.de)
TMI	Telemedizinische Infrastruktur
TTP	Trusted Third Party
UAR	Unexpected Adverse Reaction; unerwartete Nebenwirkung im Rahmen einer Arzneimittelprüfung
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (www.datenschutzzentrum.de)
UML	Unified Modeling Language (www.uml.org)
VK	Versichertenkarte
VOMS	Virtual Organization Membership Service
VPN	Virtual Private Network
W3C	World Wide Web Consortium (www.w3.org)
WHO	World Health Organization (www.who.org)
Wiki	Webseitensammlung, die nicht nur per Browser gelesen, sondern auch online geändert werden kann. Der Name ist von „wikiwiki“, dem hawaiianischen Wort für „schnell“, abgeleitet.
XACML	eXtensible Access Control Markup Language: Vom OASIS-Konsortium standardisiertes XML-Schema zur Darstellung und Verarbeitung von Autorisierungs-Policies
XML	extensible Markup Language

Literatur

1) Reng, C.-M. et al. (2006). Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin: Im Auftrag des Koordinierungsrates der Telematikplattform für Medizinische Forschungsnetze. (1. Aufl.), Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft.
2) Becker, R. et al. Ein generisches Datenschutzkonzept für Biomaterialbanken (Version 1.0). http://www.tmf-ev.de/produkte/P010021 Letzter Zugang: 2014–06–10.
3) Prokosch, H.-U. (2010). Single-Source-Aktivitäten in Deutschland. mdi **12** (2): S. 56–57.
4) Prokosch, H.-U. und Ganslandt, T. (2009). Perspectives for medical informatics. Reusing the electronic medical record for clinical research. Methods of Information in Medicine **48** (1): S. 38–44.
5) Harnischmacher, U. et al. (2006). Checkliste und Leitfaden zur Patienteneinwilligung. (1. Aufl.), Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft.
6) EC. Europäische Kommission (2012). Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf. Letzter Zugang: 2014–06–10.
7) Pommerening, K. et al. (2008). Register zu seltenen Krankheiten – Patientencompliance und Datenschutz. Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz **51** (5): S. 491–499.
8) ICH. International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use E6(R1) (1996). Guideline for Good Clinical Practice. http://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E6_R1/Step4/E6_R1__Guideline.pdf. Letzter Zugang: 2014–06–10.
9) Dierks, C. (2010). Rechtsgutachten zur elektronischen Archivierung. Teil 2: Spezifische Rechtsfragen zur elektronischen Aufbewahrung von Dokumenten und Dateien in klinischen Studien. TMF http://www.tmf-ev.de/produkte/P042011. Letzter Zugang: 2014–06–10.
10) Geis, I. (2010). Rechtsgutachten zur elektronischen Archivierung. Teil 1: Grundlegende Rechtsfragen zur elektronischen Aufbewahrung von Dokumenten und Dateien. TMF http://www.tmf-ev.de/produkte/P042011. Letzter Zugang: 2014–06–11.
11) Roßnagel, A. et al. (2009). Rechtsgutachten zum Datenschutz in der medizinischen Forschung. Teil 2: Gutachten zur Mitnutzung von Versorgungsdaten und zur elektronischen Gesundheitskarte nach § 291a SGB V. TMF http://www.tmf-ev.de/produkte/P039031. Letzter Zugang: 2014–06–10.
12) BSG. Bundessozialgericht: Urteil vom 10.12.2008, B 6 KA 37/07 R. Im Internet: https://sozialgerichtsbarkeit.de/sgb/esgb/show.php?modul=esgb&id=87990. Letzter Zugang: 2014–06–11.
13) DGEpi. Deutsche Gesellschaft für Epidemiologie (DGEpi) (2008). Leitlinien und Empfehlungen zur Sicherung Guter Epidemiologischer Praxis (GEP). http://dgepi.de/fileadmin/pdf/leitlinien/GEP_mit_Ergaenzung_GPS_Stand_24.02.2009.pdf. Letzter Zugang: 2014–06–11.
14) NER. Nationaler Ethikrat (2004). Biobanken für die Forschung. http://www.ethikrat.org/dateien/pdf/NER_Stellungnahme_Biobanken.pdf. Letzter Zugang: 2014–06–11.
15) Ethikrat. Deutscher Ethikrat (2010). Humanbiobanken für die Forschung. http://www.ethikrat.org/dateien/pdf/stellungnahme-humanbiobanken-fuer-die-forschung.pdf. Letzter Zugang: 2014–06–11.
16) Dammann, U. (2006). § 3 Weitere Begriffsbestimmungen. In: Simitis, S., Hrsg. Bundesdatenschutzgesetz. S. 263 (6. Aufl.), Baden-Baden: Nomos.
17) Bizer, J. (2006). BDSG Kommentar § 3 Pseudonymisieren. In: Simitis, S., Hrsg. Bundesdatenschutzgesetz. S. 313–315 (6. Aufl.), Baden-Baden: Nomos.
18) Simitis, S., Hrsg. (2006). Bundesdatenschutzgesetz. (6. Aufl.), Baden-Baden: Nomos.
19) Metschke, R. und Wellbrock, R. (2002). Datenschutz in Wissenschaft und Forschung. Berliner Beauftragter für Datenschutz und Informationsfreiheit http://www.datenschutz-berlin.de/attachments/47/Materialien28.pdf. Letzter Zugang: 2014–06–11.
20) Dierks, C. (2008). Rechtsgutachten zur elektronischen Datentreuhänderschaft. TMF http://www.tmf-ev.de/produkte/P052011. Letzter Zugang: 2014–06–11.

21) EC. Europäische Kommission (2012). Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG. http://ec.europa.eu/health/files/clinicaltrials/2012_07/proposal/2012_07_proposal_de.pdf. Letzter Zugang: 2014–06–11.

22) Dierks, C. (2009). Rechtsgutachten zum Datenschutz in der medizinischen Forschung. Teil 1: Pseudonymisierungsverpflichtung bei Anwendungsfällen mit gleichzeitigem Versorgungs- und Forschungsbezug und Fragen zur Relevanz des Medizinproduktegesetzes (MPG). TMF http://www.tmf-ev.de/produkte/P039031. Letzter Zugang: 2014–06–11.

23) Simon, J.W. et al. (2006). Biomaterialbanken – Rechtliche Rahmenbedingungen. Schriftenreihe der Telematikplattform für Medizinische Forschungsnetze. (1. Aufl.), Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft.

24) Bdtag. Deutscher Bundestag (2002). Schlussbericht der Enquete-Kommission Recht und Ethik der modernen Medizin. http://dip21.bundestag.de/dip21/btd/14/090/1409020.pdf. Letzter Zugang: 2014–06–11.

25) Duttge, G. (2010). Das Recht auf Nichtwissen in der Medizin. Datenschutz und Datensicherheit – DuD **34** (1): S. 34–38.

26) WMA. World Medical Association (2008). Deklaration von Helsinki. http://www.bundesaerztekammer.de/downloads/DeklHelsinki2008.pdf. Letzter Zugang: 2014–06–11.

27) Schütze, B. und Oemig, F. (2010). Poster: Nutzung von Patientendaten zur Forschung und Qualitätssicherung – Datenschutzrechtliche Fragestellungen. Vortrag im Rahmen von: 55. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS), Mannheim.

28) DSK. AK Technik und Medien: Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2011). Orientierungshilfe – Cloud Computing. http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf. Letzter Zugang: 2014–06–11.

29) EuGH. Urteil des Europäischen Gerichtshofs vom 9. März 2010 – Europäische Kommission/Bundesrepublik Deutschland (Rechtssache C-518/07). Im Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:113:0003:0004:DE:PDF. Letzter Zugang: 2014–06–11.

30) DSK. Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 in Würzburg: Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze. http://www.datenschutz-berlin.de/attachments/757/TOP-6-KV-SafeNet.pdf. Letzter Zugang: 2014–06–11.

31) ICH. International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (2005). E2B(R) Clinical Safety Data Management: Data Elements for Transmission of Individual Case Safety Reports. http://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm129399.pdf. Letzter Zugang: 2014–06–11.

32) Sloan, J.A. et al. (2007). The Mayo Clinic manuscript series relative to the discussion, dissemination, and operationalization of the Food and Drug Administration guidance on patient-reported outcomes. Value Health **10 Suppl 2**, S. S59–63.

33) Burgardt, C. (2005). Gutachten zur Sponsorverantwortung. TMF http://www.tmf-ev.de/Produkte/P000031. Letzter Zugang: 2014–06–11.

34) Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **10** (05): S. 557–570.

35) ICO. UK Information Commissioner's Office (2012). Anonymisation: managing data protection risk code of practice. http://ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf. Letzter Zugang: 2014–06–11.

36) Murphy, S.N. et al. (2007). Architecture of the open-source clinical research chart from Informatics for Integrating Biology and the Bedside. AMIA Annu Symp Proc S. 548–552.

37) DSK. Arbeitskreis Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2012). Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur. Orientierungshilfe Mandantenfähigkeit. http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Mandantenf%C3%A4higkeit.pdf. Letzter Zugang: 2014–06–11.

38) Schneier, B. (2007). Basketball Referees and Single Points of Failure. Schneier on Security http://www.schneier.com/blog/archives/2007/09/basketball_refe.html. Letzter Zugang: 2014–06–11.

39) BMBF. Bundesministerium für Bildung und Forschung (2003). Gesundheitsforschung: Forschung für den Menschen. Seltene Erkrankungen – Millionen Patienten. Dokumentation des Presseworkshops am 11.11.2003. http://www.bmbf.de/pub/seltene_erkrankungen_flyer.pdf. Letzter Zugang: 2014–06–11.

40) DKKR. Deutsches Kinderkrebsregister. http://www.kinderkrebsregister.de/. Letzter Zugang: 2014–06–11.

41) Creutzig, U. et al. (2003). Krebserkrankungen bei Kindern: Erfolg durch einheitliche Therapiekonzepte seit 25 Jahren. Deutsches Ärzteblatt **100** (13): S. 842–852.

42) Weichert, T. (2010). Cloud Computing und Datenschutz. Datenschutz und Datensicherheit – DuD **34** (10): S. 679–687.

43) Freitag, S. (2011). Rechnen lassen. Rechnen im Netz: Grid versus Cloud. ix **8**, S. 94–97.

44) Knösel, J. (2007). Der Clinical Data Manager EDC. Forum der Medizin-Dokumentation und Medizin-Informatik **2**, S. 62–64.

45) Sens, B. und Fischer, B. (2003). GMDS-Arbeitsgruppe Qualitätsmanagement in der Medizin: Begriffe und Konzepte des Qualitätsmanagements. Informatik, Biometrie und Epidemiologie in Medizin und Biologie **34** (1): S. 1–61.

46) Baun, C. et al. (2007). Kennzeichen D. D-Grid schafft Grundlage für e-Science. ix **12**, S. 104–107.

47) Sax, U. et al., Hrsg. (2007). Grid-Computing in der biomedizinischen Forschung. Datenschutz und Datensicherheit. (1. Aufl.), München: Urban & Vogel.

48) Pschyrembel, Hrsg. (2002). Klinisches Wörterbuch. (259. Aufl.), Berlin: Walter De Gruyter.

49) Bundesärztekammer (1996). Empfehlungen zu ärztlicher Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Deutsches Ärzteblatt **93** (43): S. A2809–A2812.

50) BVerfGE. Bundesverfassungsgericht 65,1 – Volkszählung. Urteil des Ersten Senats vom 15.12.1983. Im Internet: http://www.datenschutz.rlp.de/downloads/bverfge_65_1_-_volkszaehlung.pdf. Letzter Zugang: 2014–06–11.

Anhang

Weiterführende Informationen und Materialien der TMF zum Thema stehen unter www.tmf-ev.de/datenschutz-leitfaden zur Verfügung.

TMF – Forscher vernetzen, Lösungen bereitstellen, Doppelarbeit vermeiden

Die TMF sorgt für Qualitäts- und Effizienzsteigerung in der medizinischen Forschung

Die moderne medizinische Forschung steht vor zunehmend komplexen Herausforderungen, für deren Lösung sich die Akteure aus Grundlagenforschung, klinischer Forschung, Versorgungseinrichtungen, Industrie und weiteren Partnern miteinander vernetzen und gemeinsame Strategien entwickeln müssen. Ein zentraler Ansatz ist die Effizienzsteigerung auf allen Ebenen der medizinischen Forschungs- und Entwicklungskette, um – bei gesicherter Qualität – Forschungsergebnisse auf schnellstem Wege in die Patientenversorgung zu übertragen und damit zu einem effizienten und leistungsfähigen Gesundheitswesen beizutragen. Die Bundesregierung unterstützt diesen Prozess unter anderem im Rahmen des Gesundheitsforschungsprogramms und fördert seit mehr als zehn Jahren konsequent die medizinische Verbundforschung. Erfolgreiche Beispiele sind die herausragenden Ergebnisse aus den Kompetenznetzen in der Medizin oder den Koordinierungszentren für Klinische Studien.

Die TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung (kurz: TMF), die vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wird, leistet hierzu einen entscheidenden Beitrag, indem sie Forscher Disziplin-übergreifend zusammenbringt und Lösungen für die vernetzte medizinische Forschung bereitstellt. Damit übernimmt sie eine wesentliche nationale Aufgabe zur Qualitäts- und Effizienzsteigerung für die Forschung.

Ziele und Aufgaben

Als Dachorganisation für die medizinische Verbundforschung verfolgt die TMF das Ziel, die organisatorischen, rechtlichen-ethischen und technologischen Voraussetzungen für die klinische, epidemiologische und translationale Forschung zu verbessern. Sie hat die Aufgabe, die wissenschaftliche Arbeit der modernen medizinischen Forschung, die heutzutage überwiegend in kooperativen Projekten mit mehreren beteiligten Standorten stattfindet, zu unterstützen. Dazu stellt sie – öffentlich und gemeinfrei, also für jeden Forscher nutzbar – Gutachten, generische Konzepte, Leitfäden und IT-Anwendungen ebenso wie Schulungs- und Beratungsangebote bereit. Der überwiegende Teil der Produkte steht unter www.tmf-ev.de zum Download zur Verfügung. Ausgewählte Ergebnisse werden in der Schriftenreihe der TMF publiziert.

Die Produkte werden – von der Forschung für die Forschung – von den Fachexperten der Mitgliedsverbünde entwickelt, die in den interdisziplinären Arbeitsgruppen der TMF zusammenkommen. Als Grundmuster und Leitmotiv der gemeinsamen Arbeit in den Arbeitsgruppen gilt der Anspruch, gemeinsame Probleme gemeinsam zu lösen, von vorhandenen Erfahrungen gegenseitig zu profitieren, Doppelarbeit zu vermeiden sowie professionelle Lösungen zu erarbeiten, zu diesen einen Konsens in der Forschergemeinschaft herzustellen und ihre konsequente Nutzung und langfristige Verfügbarkeit zu gewährleisten.

Geschichte

Die TMF wurde 1999 unter dem Namen „Telematikplattform für Medizinische Forschungsnetze“ als Förderprojekt des BMBF gegründet. Mit dem Ziel, die Struktur zu verstetigen und die gemeinsame Querschnittseinrichtung der medizinischen Verbundforschung noch stärker in die Hände der Forscher selbst zu legen, wurde 2003 der TMF e.V. gegründet. Seither ist die Zahl der Mitgliedsverbünde stark angewachsen. Damit zusammenhängend hat sich auch das thematische Spektrum der TMF verbreitert, die zunächst primär auf Fragen der IT-Infrastruktur ausgerichtet war. Die Themen reichen heute von rechtlichen und ethischen Rahmenbedingungen und Fragen der IT-Infrastruktur über Qualitätsmanagement und Standards für klinische Studien sowie den Themenkomplex Biobanken und molekulare Medizin bis hin zum Problem der Verzahnung von Forschung und Versorgung oder Fragen der Verbundkoordination und der Wissenschaftskommunikation.

2010 beschloss die Mitgliederversammlung eine Umbenennung der TMF, da der Begriff „Telematikplattform“ diesem breiten Spektrum nicht mehr gerecht wurde. Der seither geführte Name „TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.“ erfasst die Aufgaben und Themen der TMF auf spezifischere Weise.

Mitglieder

Mitglieder der TMF sind überregionale medizinische Forschungsverbünde, vernetzt arbeitende universitäre und außeruniversitäre Forschungsinstitute, Methodenzentren, regionale Verbundprojekte sowie kooperative Studiengruppen. Dazu gehören unter anderem

- die Deutschen Zentren der Gesundheitsforschung,
- die Nationale Kohorte,
- Kompetenznetze in der Medizin,
- Koordinierungszentren bzw. Zentren für Klinische Studien (KKS/ZKS),
- Integrierte Forschungs- und Behandlungszentren,
- Netzwerke für Seltene Erkrankungen,
- die Fraunhofer-Gesellschaft (mit dem Fraunhofer ITEM als direktem Mitglied),
- Zoonosen-Forschungsverbünde,
- zentralisierte Biomaterialbanken (Nationale Biobanken-Initiative)
- Universitätsinstitute,
- Patientenorganisationen
- und zahlreiche weitere.

Über Mitgliedsverbünde sind bundesweit alle Universitätsklinika und zahlreiche außeruniversitäre Forschungsstandorte in unterschiedlicher Weise in die TMF eingebunden. Mit Kooperationspartnerschaften sorgt die TMF auch darüber hinaus für eine Einbindung der relevanten Institutionen im Gesundheitswesen.

Themen und Arbeitsweise

Die durch die Forschungsverbünde und -einrichtungen gemeinsam zu bearbeitenden Querschnittsaufgaben gehen weit über Fragen von Informations- und Kommunikationstechnologie im technischen Sinne hinaus. Die Wissenschaftler in den Forschungsprojekten brauchen Unterstützung und Erfahrungsaustausch in großer Breite:

- zu Fragen der konkreten Umsetzung von Datenschutz und ethischen Richtlinien,
- zum Aufbau von Forschungsinfrastrukturen wie Datenbanken für Forschungsregister und Biobanken,
- zur strategischen Nutzung von Informationstechnologie für die Prozessunterstützung wie für die wissenschaftliche Auswertung,
- zu Rechtsfragen in vielerlei Hinsicht, beispielsweise zum Vertragsrecht innerhalb von Netzwerken, zu Patienteneinwilligungen oder zu Verwertungsfragen,
- zu Fragen der Organisation und des Managements von Forschungsnetzen und ihren Projekten sowie
- zunehmend auch zu Fragen des Budgetmanagements, der Finanzierung und der Nachhaltigkeit von mit öffentlichen Geldern aufgebauten Netzwerkstrukturen.

Alle diese Fragen werden kontinuierlich in den Arbeitsgruppen der TMF bearbeitet, in denen sich die jeweiligen Fachleute aus den verschiedenen Projekten und Forschungsstandorten interdisziplinär zusammenfinden. Dabei entstehen strategische Anstöße und Impulse für die Forschungsinfrastruktur, vor allem aber konkrete Hilfen, Produkte und Services für den Forscher. Regelmäßig tagen einzelne Arbeitsgruppen auch gemeinsam, um auf diese Weise themenübergreifende Aspekte besser aufnehmen und Doppelaktivitäten der Arbeitsgruppen vermeiden zu können.

Arbeitsgruppen

Die Arbeitsgruppen initiieren Projekte und betreuen sie im Verlauf – bis hin zur Implementierung der Ergebnisse und zur Beratung von Forschungsprojekten auf dieser Basis. Neue Projektvorschläge durchlaufen ein mehrstufiges Auswahlverfahren – von der fachlichen Prüfung und Schärfung in den Arbeitsgruppen über Beratung in der Geschäftsstelle bis hin zur Begutachtung durch den Vorstand. Mit diesem Vorgehen wird sichergestellt, dass die in den Projekten adressierten Probleme für die Forschergemeinschaft relevant sind und dass die angestrebte Lösung einen breiten Konsens für die spätere Anwendung findet.

Arbeitsgruppen können in der TMF je nach aktuellem Bedarf neu eingerichtet, zusammengelegt oder auch aufgelöst werden, wenn ein Thema keine hohe Relevanz mehr hat. Derzeit sind neun Arbeitsgruppen aktiv:

- Arbeitsgruppe Datenschutz
- Arbeitsgruppe IT-Infrastruktur und Qualitätsmanagement
- Arbeitsgruppe Biomaterialbanken
- Arbeitsgruppe Molekulare Medizin
- Arbeitsgruppe Management Klinischer Studien
- Arbeitsgruppe Medizintechnik
- Arbeitsgruppe Zoonosen und Infektionsforschung
- Arbeitsgruppe Netzwerkkoordination
- Arbeitsgruppe Wissenschaftskommunikation

Der interdisziplinäre Austausch wird über die Arbeitsgruppen hinaus durch zahlreiche Symposien und Workshops, durch den TMF-Jahreskongress sowie durch Foren – aktuell beispielsweise zum Thema Versorgungsforschung – ergänzt.

Lösungen stehen frei zur Verfügung

Die TMF stellt Gutachten, generische Konzepte, Leitfäden und IT-Anwendungen ebenso bereit wie sie Schulungs- und Beratungsservices der Arbeitsgruppen, auch in Form von Einzelberatungen, anbietet. Die Ergebnisse der Arbeit in der TMF stehen öffentlich und gemeinfrei zur Verfügung.

Mit diesem offenen Ansatz verfolgt die TMF das Ziel,

- methodisches Know-how und Infrastrukturen für die vernetzte medizinische Forschung breit verfügbar zu machen,
- die Harmonisierung, die Interoperabilität und das Qualitätsmanagement in der vernetzten medizinischen Forschung durch entsprechende Infrastruktur, Leitfäden und Services zu stärken,
- die Kollaboration in der deutschen medizinischen Forschung sowie deutsche Forscher in internationalen Kooperationen zu stärken,
- die Verstetigung und Nachhaltigkeit akademischer medizinischer Forschungsprojekte zu unterstützen und
- einen Beitrag zu sinnvollem Mitteleinsatz in der öffentlich geförderten medizinischen Forschung zu leisten, indem sie Doppelentwicklungen vermeiden hilft und die Wiederverwendung vorhandener Lösungen organisiert.

Mit ihren Lösungen adressiert die TMF vor allem die nicht-kommerzielle, akademische – universitäre wie außeruniversitäre – Forschung in Deutschland. Unabhängig davon ist aber auch ein steigendes Interesse an den Angeboten aus der Industrie zu verzeichnen. Viele Lösungen der TMF sind zudem auch für das Ausland, insbesondere die deutschsprachigen Länder, relevant und werden in dortigen Forschungseinrichtungen bereits genutzt.

Alle Download-geeigneten Produkte und Ergebnisse stehen auf der TMF-Website zur Verfügung. Einzelne Software-Werkzeuge sind sehr komplex und be-

dürfen einer individuellen Anpassung und Erläuterung, so dass sie nur über den direkten Kontakt zur TMF-Geschäftsstelle erhältlich sind, die dann auch für die Betreuung bei der Implementierung und Nutzung des Produktes sorgt. Darüber hinaus fließen die Ergebnisse kontinuierlich auch in die Diskussionen in den Arbeits- und Projektgruppen ein, und sie werden in konkreten Beratungsgesprächen sowie in Schulungs- und Informationsveranstaltungen vermittelt.

TMF-Schriftenreihe

Wichtige Konzepte, Leitfäden und Hilfstexte veröffentlicht die TMF in ihrer Schriftenreihe, die sie seit mehreren Jahren bei der Medizinisch Wissenschaftlichen Verlagsgesellschaft herausgibt. So erschienen 2006 als erster Band die generischen Lösungen zum Datenschutz für die Forschungsnetze in Buchform (Reng et al.: Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin, Berlin 2006 – Bd. 1). In der Zwischenzeit sind diese Konzepte einer grundlegenden Revision unterzogen und erneut mit den Bundes- und Landesdatenschützern abgestimmt worden. Die überarbeiteten Konzepte werden mit dem vorliegenden Leitfaden als Band 11 der TMF-Schriftenreihe für einen breiten Nutzerkreis verfügbar gemacht (Pommerening et al.: Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, Berlin 2014 – Bd. 11).

Es folgte das Rechtsgutachten zum Aufbau und Betrieb von Biomaterialbanken (Simon et al.: Biomaterialbanken – Rechtliche Rahmenbedingungen, Berlin 2006 – Bd. 2), das im Februar 2008 um einen weiteren Band zum Thema Qualitätssicherung von Biobanken ergänzt wurde (Kiehntopf/Böer: Biomaterialbanken – Checkliste zur Qualitätssicherung, Berlin 2008 – Bd. 5). Das Datenschutzkonzept, das ursprünglich als Bd. 6 der Schriftenreihe publiziert werden sollte, ist in die vorliegende Publikation der neuen Datenschutzkonzepte integriert worden.

Mit der Checkliste zur Patienteneinwilligung legte die TMF Ende 2006 ein Referenzwerk vor, das den Anwendern ermöglicht, auf der Basis von relevanten, dokumentierten und kommentierten Quellen Patienteninformationen und Einwilligungserklärungen für klinische Studien zu erstellen, die den regulatorischen Anforderungen entsprechen (Harnischmacher et al.: Checkliste und Leitfaden zur Patienteneinwilligung, Berlin 2006 – Bd. 3). Wie die meisten anderen Buchpublikationen auch, wird dieser Band durch weitere online verfügbare Materialien (z.B. Musterverträge) oder Services ergänzt.

2007 erschien die erste Auflage der Leitlinie zur Datenqualität in der medizinischen Forschung, die 2014 in einer aktualisierten und ergänzten Fassung neu aufgelegt worden ist. Die Leitlinie (Nonnemacher et al.: Datenqualität in der medizinischen Forschung, Berlin 2014 – Bd. 4) enthält Empfehlungen zum Management von Datenqualität in Registern, Kohortenstudien und Data Repositories.

Ein Rechtsgutachten zum Problemfeld der Verwertungsrechte in der medizinischen Forschung (Goebel/Scheller: Verwertungsrechte in der medizinischen Forschung, Berlin 2008 – Bd. 7) erschien 2008 als erste Veröffentlichung einer Reihe von Rechtsgutachten, die die TMF zu verschiedenen Fragen hat erstellen lassen, unter anderem zum Thema „elektronische Archivierung von Studienunterlagen". Die Publikation dieser weiteren Rechtsgutachten in der TMF-Schriftenreihe wird sukzessive folgen.

Mit Band 8 (Mildner [Hrsg.]: Regulatorische Anforderungen an Medizinprodukte, Berlin 2011 – Bd. 8) hat die TMF 2011 erneut die Aufarbeitung eines im Umbruch befindlichen Feldes vorgelegt. Das Buch bietet eine Einführung in den regulatorischen Prozess bei der Entwicklung von Medizinprodukten und stellt Handlungshilfen bereit. Dabei wird der gesamte Bereich von der klinischen Bewertung bis zum Health Technology Assessment abgedeckt.

Praktische Empfehlungen für die Verarbeitung und Analyse von Daten, die bei der Hochdurchsatz-Genotypisierung anfallen, gibt Band 9 (Krawczak/Freudigmann [Hrsg.]: Qualitätsmanagement von Hochdurchsatz-Genotypisierungsdaten, Berlin 2011 – Bd. 9), der ebenfalls 2011 publiziert werden konnte. Dabei reichen die behandelten Fragen von Problemen der Validität und Plausibilität über die Erkennung und Vermeidung von Fehlern bis hin zu Anforderungen an Datenhaltung und Datentransfer.

An die TMF-Ergebnisse im Bereich Datenschutz und Patienteneinwilligung knüpft der 2012 erschienene Band 10 an (Goebel/Scheller: Einwilligungserklärung und Forschungsinformation zur Gewinnung tierischer Proben, Berlin 2012 – Bd. 10). Die Ergebnisse sind im Auftrag der Nationalen Forschungsplattform für Zoonosen erarbeitet worden. Sie dienen dazu, Forschenden Rechtssicherheit bei der Entnahme und Bearbeitung von Tierproben zu geben und sie bei der Erstellung der relevanten Einwilligungsunterlagen zu unterstützen.

Weitere Informationen und Kontakt

TMF – Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e.V.
Charlottenstraße 42/Ecke Dorotheenstraße
10117 Berlin
Tel.: 030 – 22 00 247–0
Fax: 030 – 22 00 247–99
E-Mail: info@tmf-ev.de
Internet: www.tmf-ev.de

Zur Schriftenreihe der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.

In der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. haben sich Netzwerke und vernetzt arbeitende Einrichtungen zusammengeschlossen, um gemeinsam die Fragestellungen und Herausforderungen von medizinischer Forschung an verteilten Standorten zu lösen und die Erfahrungen zu bündeln. Durch den Community-Ansatz erfahren die Ergebnisse der TMF eine breite inhaltliche Abstimmung in der medizinischen und medizininformatisch-biometrischen Fachwelt. Mit ihrer Schriftenreihe macht die TMF die Lösungen einer breiteren Leserschaft zugänglich.

Bisher in der Schriftenreihe erschienen:

Band 1:
Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin
von Carl-Michael Reng | Peter Debold
Christof Specker | Klaus Pommerening
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 2:
Biomaterialbanken – Rechtliche Rahmenbedingungen
von Jürgen Simon | Rainer Paslack | Jürgen Robienski
Jürgen W. Goebel | Michael Krawczak
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 3:
Checkliste und Leitfaden zur Patienteneinwilligung
Grundlagen und Anleitung für die klinische Forschung
von Urs Harnischmacher | Peter Ihle | Bettina Berger
Jürgen Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 4, 2. Auflage:
Datenqualität in der medizinischen Forschung
von Michael Nonnemacher | Daniel Nasseh
Jürgen Stausberg
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2014

Band 5:
Biomaterialbanken – Checkliste zur Qualitätssicherung
von Michael Kiehntopf | Klas Böer
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2008

Band 7:
Verwertungsrechte in der vernetzten medizinischen Forschung
von Jürgen W. Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2009

Band 8:
Regulatorische Anforderungen an Medizinprodukte
von Kurt Becker | Sandra Börger | Horst Frankenberger
Dagmar Lühmann | Thomas Norgall
Christian Ohmann | Annika Ranke | Reinhard Vonthein
Andreas Ziegler | Andreas Zimolong
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2011

Band 9:
Qualitätsmanagement von Hochdurchsatz Genotypisierungsdaten
von Michael Krawczak | Mathias Freudigmann (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2011

Band 10:
Einwilligungserklärung und Forschungsinformation zur Gewinnung tierischer Proben
von Jürgen W. Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2012